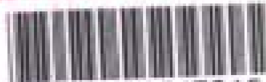
http://maths352.bokee.com
00128620
01-K9
30

数学游戏与欣赏

[英国]劳斯·鲍尔 [加拿大]考克斯特著 杨应辰等译

· 上海教育出版社

2006.07.09
齐建民



我们必须知道，而且我们必将知道

VISIT…

LANZAROTE
Caliente.com

http://maths352.bokee.com

W. W. Rouse Ball, H. S. M. Coxeter

Mathematical Recreations & Essays

University of Toronto Press

© Trinity College, Cambridge, 1974

根据多伦多大学出版社 1974 年第 12 版译出，

本书中文版权由上海市版权代理公司帮助取得

图书在版编目(CIP)数据

数学游戏与欣赏/(英)鲍尔,(加拿大)考克斯特著;杨应辰,蒋正新译. 一上海:上海教育出版社,2001.4

(通俗数学名著译丛/史树中,李文林主编)

ISBN 7-5320-7094-8

Ⅰ.数... Ⅱ.①鲍...②考...③杨...④蒋...

Ⅲ.数学-通俗读物 Ⅳ.01-49

中国版本图书馆 CIP 数据核字(2000)第 42468 号

通俗数学名著译丛

数学游戏与欣赏

[英国] 劳斯·鲍尔

[加拿大] 考克斯特 著

杨 应 辰 等译

上海世纪出版集团
上 海 教 育 出 版 社 出版发行

(上海永福路 123 号 邮政编码:200031)

各地新华书店经销 上海商务联西印刷厂印刷

开本 850×1156 1/32 印张 14.5 插页 4 字数 342,000

2001 年 4 月第 1 版 2001 年 4 月第 1 次印刷

印数 1—5,250 本

ISBN 7-5320-7094-8/G·7250 定价:(软精)25.70 元

我们必须知道，而且我们必将知道

http://maths352.bokee.com

译丛序言

数学，这门古老而又常新的科学，正阔步迈向21世纪.

回顾即将过去的世纪，数学科学的巨大发展，比以往任何时代都更牢固地确立了它作为整个科学技术的基础的地位.数学正突破传统的应用范围向几乎所有的人类知识领域渗透，并越来越直接地为人类物质生产与日常生活作出贡献.同时，数学作为一种文化，已成为人类文明进步的标志.因此，对于当今社会每一个有文化的人士而言，不论他从事何种职业，都需要学习数学，了解数学和运用数学.现代社会对数学的这种需要，在未来的世纪中无疑将更加与日俱增.

另一方面，20世纪数学思想的深刻变革，已将这门科学的核心部分引向高度抽象化的道路.面对各种深奥的数学理论和复杂的数学方法，门外汉往往只好望而却步.这样，提高数学的可接受度，就成为一种当务之急.尤其是当世纪转折之际，世界各国都十分重视并大力加强数学的普及工作，国际数学联盟(IMU)还专门将2000年定为**“世界数学年”**，其主要宗旨就是“使数学及其对世界的意义被社会所了解，特别是被普通公众所了解”.

一般说来，一个国家数学普及的程度与该国数学发展的水平相应并且是数学水平提高的基础.随着中国现代数学研究与教育的长足进步，数学普及工作在我国也受到重视.早在60年代，华罗庚、吴文俊等一批数学家亲自动手撰写的数学通俗读

我们必须知道，而且我们必将知道

http://maths352.bokee.com

物,激发了一代青少年学习数学的兴趣,影响绵延至今.改革开放以来,我国数学界对传播现代数学又作出了新的努力.但总体来说,我国的数学普及工作与发达国家相比尚有差距.我国数学要在下世纪初率先赶超世界先进水平,数学普及与传播方面的赶超乃是一个重要的环节和迫切的任务.为此,借鉴外国的先进经验是必不可少的.

《通俗数学名著译丛》的编辑出版,正是要通过翻译、引进国外优秀数学科普读物,推动国内的数学普及与传播工作,为我国数学赶超世界先进水平的跨世纪工程贡献力量.丛书的选题计划,是出版社与编委会在对国外数学科普读物广泛调研的基础上讨论确定的.所选著述,基本上都是在国外已广为流传、受到公众好评的佳作.它们在内容上包括了不同的种类,有的深入浅出介绍当代数学的重大成就与应用;有的循循善诱启迪数学思维与发现技巧;有的富于哲理阐释数学与自然或其他科学的联系;等等,试图为人们提供全新的观察视角,以窥探现代数学的发展概貌,领略数学文化的丰富多采.

丛书的读者对象,力求定位于尽可能广泛的范围.为此丛书中适当纳入了不同层次的作品,以使包括大、中学生;大、中学教师;研究生;一般科技工作者等在内的广大读者都能开卷受益.即使是对于专业数学工作者,本丛书的部分作品也是值得一读的.现代数学是一株分支众多的大树,一个数学家对于他所研究的专业以外的领域,也往往深有隔行如隔山之感,也需要涉猎其他分支的进展,了解数学不同分支的联系.

需要指出的是,由于种种原因,近年来国内科技译著尤其是科普译著的出版并不景气,有关选题逐年减少,品种数量不断下降.在这样的情况下,上海教育出版社以迎接2000世界数学年为契机,按照国际版权公约,不惜耗资购买版权,组织翻译出版这套《通俗数学名著译丛》,这无疑是值得称道和支持的举措.参加本丛书翻译的专家学者们,自愿抽出宝贵的时间来进行这类

我们必须知道，而且我们必将知道

http://maths352.bokee.com



通常不被算作成果但却能帮助公众了解和欣赏数学成果的有益工作，同样也是值得肯定与提倡的.

像这样集中地翻译、引进数学科普读物，在国内还不多见.我们热切希望广大数学工作者和科普工作者来关心、扶植这项工作，使《通俗数学名著译丛》出版成功.

让我们举手迎接2000世界数学年，让公众了解、喜爱数学，让数学走进千家万户！

《通俗数学名著译丛》编委会

1997年8月

我们必须知道，而且我们必将知道

http://maths352.bokee.com

译者序

劳斯·鲍尔(W. W. Rouse Ball)的《数学游戏与欣赏》是一部名著，自1892年初版后，再版修订十二次并又重印已十几次，足见其广受西方大众及学者的赏识与欢迎，盛誉经久不衰.氏是这方面的专家，广见多闻，博古通今，著作还有多种深浅不同的数学游戏小册子.它们的问世，对引发学子对数学的兴趣，起着不小的作用.可惜这些著作一向未被介绍到国内.这本书于1938年经考克斯特(H.S.M.Coxeter)再次作大量增修，特别是末一章"密码术与破译"由美国作战部专家辛科夫(A.Sinkov)重写，使之大为增色.

为此，我们认为，将它译为中文出版，实补国内科普资料的一个空白，而对国人之数学爱好必将有所促进，对青年们科学思维能力之培养也将起积极的作用.

译者不揣谫陋，担任移译.由于原著曾经过不止一人的补充与改写，格调难以完全一致.涉及的问题浅者小学生可以理解，难题虽专家也赞许其深入浅出，点到了好处.有些地方讲得十分详细，另一些地方又只一笔带过，而总体上却常保持着聊天的韵味.特别是引经据典之处往往不易查究，冷僻怪字间出，用意颇需推敲.为了保持原著的风格而又便于读者理解其内容，译者尽力作了多方面的考证.从印度的史诗到希腊的古币，不获指引，难见端倪.简略难明之处做了不少的注释.如能帮助读者理解真谛而感到兴趣，那就是译者的莫大欣慰了.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

本书除第10章初稿曾由蒋正新执笔外，其余移译工作均由杨应辰担任并校正全文．限于我们的水平，乖谬在所难免．倘蒙读者指正，则一字之师亦当永怀不忘也．

译　者

于北京航空航天大学

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第 10 版原序

本书包括通常称为数学游戏的各种问题的阐述和一些关于此类问题的赏析.我排除了一切涉及高等数学的材料.要指出,许多论断未必有什么实际用处,而且大部分结果也不是新的.有言在先,那么读者往下看的时候当不会见怪.从另一方面说,这里讨论的许多问题都是很有趣的,其中不少问题与杰出的数学家的名字联系在一起.一些引用的文章对于英语读者来说,至今还是不容易找到的.这次出版增添了自 1892 年本书初版以来出现的许多新材料.

现在的这本书包含十六章,其论题如目录所示.前四章中所述的问题似不足道.任何一般的英语著作中都有所论述.我本可略过它们而让读者去看别的书,可是考虑到没有那些书的读者,所以还是把它们插进去为好.熟悉它们的读者可以完全跳过它们,如果有点舍不得,也可浏览一下.还要补充一句,对于那些详细解答太长或太繁的问题,一般地,我只给出一些例子而指出论述详尽解法的文章或书籍.有时我也介绍一些尚待解决的问题.

对各种问题的来源和所给的解均注明了就我所知的详尽的参考资料.凡是仅给定理的结论的时候,我总指出可以找到证明的权威著作.一般地,除非另行声明,参考资料都是从原著中摘取来的;不过,虽然也曾花了不少时间去查对它们,我不敢说一点错误或刊误都没有.

劳斯·鲍尔

我们必须知道,而且我们必将知道

http://maths352.bokee.com

第11版原序

在修订劳斯·鲍尔的令人喜爱的小书的时候，我的原则是在保留其风格的前提下，补充他本人也会喜爱的材料．和几位数学家磋商之后，我觉得删掉原书第10版中的第5，第8和第15章为好．（关于“绳图”请参看第9版或第10版，或看劳斯·鲍尔的关于这个题目的小册子．）第12章被拆开而分散到第1，第3，第4与第11章中去了．

现在的第5章是新的；第2章与第8章的大部分，还有第3章与第7章的相当大一部分也都是新的．此外，第14章关于密码术与破译，也由美国国防部破译专家辛科夫（A．Sinkov）完全重新改写．我向他和许多协助者特别是雷默（D．H．Lehmer）表示衷心的感谢，他建设性地评审了手稿的第2章；还有安德烈斯（J．M．Andreas），他提供了第5章的一些图；还有唐奇安（P．S．Donchian），本书转载了他的模型的照片（第136页及第140页）．

H·S·M·考克斯特

1938年元月

多伦多大学

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第 12 版原序

本书初版(名称略有不同,题名为数学游戏与问题)问世恰好已八十年了.此次新版之得以再刊,要感谢多伦多大学出版社,也要感谢许多给我很大协助的朋友们和同事们,特别是乔克(J.H.H.Chalk),他审订了素数分布(第 2 章);雷默、米勒(J.C.P.Miller)和塞尔弗里奇(J.Selfridge),他指引我去参看关于大数分解因子的最新著作;小坎宁安(F. Cunningham Jr.)提供了关于挂谷宗一问题(第 3 章)的新资料;富特(R.M.Foote)与卡尼(E.J.A.Kani)查实了参考资料,提出了有益的建议并编写了多米诺(Polyominoes)那一节(第 4 章);塔特(W.T.Tutte)将图论(第 9 章)刷新了;戴维斯(C.Davis)与克努特(D.Knuth)编写了很新颖的一节"龙纹图";此外还有赛德尔(J.J.Seidel),他担任了艰难的工作——将劳斯·鲍尔的第 10 章(关于柯克曼的女学生问题)换为丰富而易读的组合理论引论,包含着他本人创始的一些概念.

从 1939 年第 11 版问世以来,电子计算机的出现将一些算术运算变得非常容易.虽然两千年前欧几里得已经发现素数有无穷多个,但直到 1877 至 1947 年间确切知道的最大素数还只是 $2^{127}-1$.此后,雷默及其他一些人借助于计算机找到了位数为几千的特定素数.然而数学家没有把计算机看成弗兰肯斯坦(Frankenstein)的精灵,因为仍然有些算术问题(如封里所示的那一个)是在计算机上求解失败之后由数学天才解决的.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



第8章的一部分已经改写，为的是显扬林格尔(G.Ringel)博士和扬斯(J.W.T.Youngs)教授在多连通曲面上染色问题的突破.为迷宫引路的特雷莫(Tremaux)规则(第9章)已经换为较好的塔里(G.Tarry.)规则.π 的处理(第12章)已经在很多地方纠正了.最后指出，根据爱丁堡的前任教授艾特肯(A.C.Aitken)的简短的传记，充实了关于计算神童的短篇.

可以看到，很多章节都是用第一人称单数的口气写的.在绝大多数情况下，读者不妨认为"我"指的就是主编劳斯·鲍尔.

欢迎读者来函指正任何错误或不清楚的地方.

H·S·M·考克斯特

1972年于

多伦多大学

我们必须知道，而且我们必将知道

http://maths352.bokee.com

目　录

译丛序言
译者序
第10版原序
第11版原序
第12版原序

第1章　算术游戏 …… 3
猜出一个人所想的数 …… 4
什么都不问、早已知结论 …… 8
涉及两个数的游戏 …… 10
取决于记数制的游戏 …… 11
十进制数的其他有趣问题 …… 13
拼凑问题 …… 15
四个数码的问题 …… 15
四个4的问题 …… 15
一组有编号物品的问题 …… 16
算式补码 …… 19
日历问题 …… 25
中世纪的算术问题 …… 26
拓荒问题 …… 31
约瑟夫斯问题 …… 31

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

尼姆游戏与类似的游戏 …… 35
穆尔游戏 …… 37
凯尔斯游戏 …… 38
威索夫游戏 …… 38
附录 …… 39
第2章 算术趣谈 …… 41
算术谬论 …… 41
第二张幺的悖论 …… 44
圣彼得堡悖论 …… 45
其他概率问题 …… 46
重排 …… 46
杂题 …… 48
排列问题 …… 49
投票问题 …… 49
圆桌骑士 …… 49
入席问题 …… 50
巴协的砝码问题 …… 50
$1/n$ 的十进制小数表示 …… 53
小数与连分式 …… 54
有理直角三角形 …… 57
三角形数与金字塔数 …… 59
可除性 …… 60
素数定理 …… 63
默森数 …… 65
完全数 …… 67
费马数 …… 69
费马最后定理 …… 71
伽罗瓦域 …… 74
第3章 几何趣谈 …… 78

我们必须知道，而且我们必将知道

http://maths352.bokee.com

几何谬论 …… 78
几何悖论 …… 86
连分式与格点 …… 88
几何剖分 …… 90
毕达哥拉斯剖分 …… 90
蒙蒂克拉剖分 …… 91
多边形的剖分 …… 92
最小剖分 …… 94
巧剖 …… 94
麦考利的四块剖分 …… 95
立体剖分 …… 96
二倍立方体 …… 96
割圆术 …… 97
仅用圆规作图 …… 99
五圆覆盖 …… 100
勒贝格极小问题 …… 102
挂谷宗一极小问题 …… 102
补记 …… 105
第 4 章　几何游戏 …… 106
静态的布局游戏 …… 106
三子成行 …… 106
p 子成行 …… 108
拼砌 …… 108
半条反拼砌 …… 110
多米诺(超级骨牌) …… 113
彩色立方体问题 …… 117
剖矩成方 …… 118
动态的布局游戏 …… 120
调车问题 …… 120

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

摆渡问题…………………………………………………… 121
测地线……………………………………………………… 123
单行棋子游戏……………………………………………… 125
一盘棋子游戏(兵卒问题)………………………………… 127
下棋问题…………………………………………………… 130
立交环……………………………………………………… 130
附录………………………………………………………… 132
第5章　多面体…………………………………………… 134
对称性与对称体…………………………………………… 134
五个柏拉图体……………………………………………… 135
开普勒的玄秘说…………………………………………… 138
帕普斯的顶点分布………………………………………… 139
复合体……………………………………………………… 141
阿基米德体………………………………………………… 142
斯托特夫人作图法………………………………………… 146
等边环带多面体…………………………………………… 147
开普勒－普安索多面体…………………………………… 150
59种正二十面体　………………………………………… 153
立体拼砌…………………………………………………… 154
摞球或密装………………………………………………… 156
海边的沙滩………………………………………………… 159
正海绵胞…………………………………………………… 159
四面体的旋转环…………………………………………… 161
万花筒……………………………………………………… 162
第6章　棋盘上的游戏…………………………………… 169
棋子的相对威力…………………………………………… 170
八后问题…………………………………………………… 173
最多子数问题……………………………………………… 179
最少子数问题……………………………………………… 179

我们必须知道，而且我们必将知道

http://maths352.bokee.com

棋盘上的回路 …… 182

马的回路 …… 182

王的回路 …… 192

车的回路 …… 192

象的回路 …… 193

杂题 …… 193

各种路线问题 …… 193

瓜里尼问题 …… 194

后的问题 …… 195

拉丁方 …… 195

欧拉方 …… 196

欧拉的官员问题 …… 197

欧拉立方 …… 198

第 7 章　幻方 …… 199

奇数阶的幻方 …… 200

单偶数阶的幻方 …… 202

双偶数阶的幻方 …… 204

镶边幻方 …… 205

同阶幻方的个数 …… 207

对称幻方与泛对角幻方 …… 207

德·拉·卢拜尔法则的推广 …… 209

阿尔诺方法 …… 211

马戈西安方法 …… 212

非相邻数字的幻方 …… 214

素数幻方 …… 215

二重幻方 …… 216

三重幻方 …… 217

其他幻方问题 …… 217

骨牌幻方 …… 217

我们必须知道，而且我们必将知道

http://maths352.bokee.com

正立方与正八面骰子……………………………… 219
联接六边形………………………………………… 219
幻立方…………………………………………… 221
第8章　地图染色问题……………………………… 226
四色猜想……………………………………………… 226
彼得森图……………………………………………… 229
化至标准图…………………………………………… 231
可能失败的最小地区数……………………………… 234
等价的数论问题……………………………………… 236
无边曲面……………………………………………… 236
对偶地图……………………………………………… 238
各种曲面上的地图…………………………………… 239
谷底，峰顶，鞍点…………………………………… 242
正二十面体的染色…………………………………… 243
第9章　单行线问题………………………………… 248
欧拉的问题…………………………………………… 248
一笔画法的个数……………………………………… 254
迷宫…………………………………………………… 259
树……………………………………………………… 265
哈密尔顿游戏………………………………………… 267
龙纹图………………………………………………… 271
第10章　组合设计 ………………………………… 276
一个射影平面………………………………………… 276
关联矩阵……………………………………………… 277
一个阿达玛矩阵……………………………………… 278
一例纠错码…………………………………………… 279
一例区组设计………………………………………… 280
施泰纳三元组………………………………………… 283
有限几何学…………………………………………… 286

我们必须知道，而且我们必将知道

http://maths352.bokee.com

柯克曼女学生问题 …… 293
拉丁方 …… 296
正方体和单形 …… 300
阿达玛矩阵 …… 301
图象传送 …… 303
三维空间中的等角线 …… 305
高维空间中的直线 …… 309
C 矩阵 …… 314
射影平面 …… 316
第 11 章　各种游戏 …… 318
华容道 …… 318
河内塔 …… 322
九连环 …… 323
纸牌游戏 …… 328
洗牌 …… 329
猜单张牌 …… 331
猜一组牌 …… 332
热尔岗摞物游戏 …… 334
三摞牌问题 …… 334
热尔岗的推广 …… 335
窗口里瞧 …… 339
捉老鼠，十三点 …… 341
第 12 章　三个古典的几何问题 …… 343
二倍立方体 …… 344
希波克拉蒂斯解法 …… 345
阿尔希塔斯解法 …… 346
柏拉图作图法 …… 346
梅内克缪斯解法 …… 347
阿波罗尼奥斯作图法 …… 347

我们必须知道，而且我们必将知道

http://maths352.bokee.com

狄俄克利斯作图法 …… 348

韦达作图法 …… 348

笛卡儿作图法 …… 349

格雷戈里作图法 …… 349

牛顿作图法 …… 349

三等分角 …… 349

帕普斯作图法 …… 350

笛卡儿作图法 …… 351

牛顿解法 …… 351

克莱罗解法 …… 351

沙勒解法 …… 352

化圆为方 …… 352

符号 π 的来源 …… 353

求 π 的近似值的几何方法 …… 355

印度数学家的成就 …… 356

中国数学家的成就 …… 357

阿拉伯数学家的成就 …… 357

欧洲数学家的成就 …… 358

求 π 的近似值的分析方法 …… 361

1699 年—1873 年间欧洲人的结果 …… 361

根据概率理论求 π 的近似值 …… 365

第 13 章　心算神童 …… 366

约翰·沃利斯，1616—1703 …… 367

朱迪代亚·巴克斯顿，1707—1772 …… 367

托马斯·富勒，1710—1790 …… 369

安德雷·玛利·安培，1775—1836 …… 370

卡尔·弗里德里希·高斯，1777—1855 …… 370

理查德·惠特利，1787—1863 …… 370

泽拉·科尔伯恩，1804—1840 …… 371

我们必须知道，而且我们必将知道

http://maths352.bokee.com

乔治·帕克·比德，1806—1878 …………………………… 372
亨利·蒙赛，维多·曼伽美尔 ……………………………… 377
约翰·马丁·查恰理亚斯·达泽，1824—1861 ……… 377
特鲁曼·亨利·萨福德，1836—1901 ………………… 379
乌戈·札姆博恩，帕瑞克尔·迪亚曼狄，卡尔·吕克勒 … 379
雅克·伊瑙迪，1867—? ………………………………… 380
记忆数字的不同方式……………………………………… 381
比德所用方式的分析……………………………………… 382
亚历山大·克莱格·艾特肯，1895—1967 ……………… 389
第 14 章　密码术与密码分析 ………………………………… 391
密码术体系………………………………………………… 392
换位法……………………………………………………… 393
多条密电码的对比分析法………………………………… 398
替代法……………………………………………………… 403
单字母法…………………………………………………… 405
双字母法…………………………………………………… 406
多字母法…………………………………………………… 406
复式字母法………………………………………………… 407
双密钥法…………………………………………………… 408
周期式复式字母法………………………………………… 409
非周期的复式字母法……………………………………… 410
流动密钥法………………………………………………… 410
代码法……………………………………………………… 412
密码类型的判定…………………………………………… 414
几点最后的注记…………………………………………… 416
附录：进一步研究的参考资料 …………………………… 417

索引…………………………………………………………… 419
关于本书……………………………………………………… 439

我们必须知道，而且我们必将知道

http://maths352.bokee.com

“在游戏的发明上，人们的机智不厌其高；智慧之士左右逢源.……在仅涉及数字的游戏之后，相继而来的是关于拓扑的游戏；……在关于数字和拓扑的游戏之后，接踵而至的是运动的游戏；……总之，一本全面论述数学游戏的专著的问世是大家翘首以待的.”

——摘自莱布尼茨1715年7月29日致德蒙特摩(De Montmort)的信.

(Les hommes ne sont jamais plus ingénieux que dans l'invention des jeux; l'espirit s'y trouve à son aise. ... Après les jeux qui dépendent uniquement des nombres viennent les jeux où entre la situation. ... Après les jeux où n'entrent que le nombre et la situation viendraient les jeux où entre le mouvement. ... Enfin il serait à souhaiter qu'on eût un cours entier des jeux, traités mathématiquement.)

我们必须知道，而且我们必将知道

http://maths352.bokee.com

46	57	68	70	81	02	13	24	35	99
71	94	37	65	12	40	29	06	88	53
93	26	54	01	38	19	85	77	60	42
15	43	80	27	09	74	66	58	92	31
32	78	16	89	63	55	47	91	04	20
67	05	79	52	44	36	90	83	21	18
84	69	41	33	25	98	72	10	56	07
59	30	22	14	97	61	08	45	73	86
28	11	03	96	50	87	34	62	49	75
00	82	95	48	76	23	51	39	17	64

整数从 0 到 99 的这样安排曾在 180 年中被认为是不可能的(见第 299 页).

我们必须知道，而且我们必将知道

第1章 算术游戏

我以叙述几个算术游戏来作为此书的开篇.人们谈到某些类型的数字间的关系时,经常是兴味昂然的.许多数学游戏的著作都载有一些此类问题.它们对于熟悉初等代数的人都是显然的.可是对于没学过代数的人来说,它们的魅力不亚于高等算术中深奥的命题对于数学家们的魅力.在整个这一章里我都致力于此类初等问题.

在进入正题之前,我要交待一下,这里所说的初等问题的大多数都是从以下两个来源之一取来的.一是梅齐里亚克(Meziriac)的巴协(Claude Gaspar Bachet)先生的经典著作"Problèmes plaisans et délectables",该书初版出于1612年,再版于1624年.以后的引证皆指1624年版.几个巴协问题都是从阿尔昆(Alcuin)、帕乔利(Pacioli di B.)、塔尔塔利亚(Tartaglia)和卡尔丹(G.Cardan)①的著作里取来的,并且其中有些问题出自东方,但我不打算增补这方面的参考资料.另一个来源是奥扎南(A.F. Ozanam)著的"Récréations mathematiques et physiques".原著两卷,1694年于巴黎出版,它包括了初版的大部分内容,是巴协、米多尔热(Mydorge)与勒雷雄(J.Leurechon)的著作的汇编.这一部分是优秀的,但奥扎南所增补的部分不能与之相提并论.在"Biographie Univer-

① 即发明解三次代数方程公式的意大利数学家G.Cardano.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



selle"里间接提到过于 1720,1735,1741,1778 和 1790 年相继出版
的版本.无疑,这些引证都是可靠的.不过我只见过以下几种版
[3] 本:1696 年阿姆斯特丹本,1723 年(奥扎南去世 6 年后)的三卷本
和续篇一本(第四卷),其中包括一个关于难题的附录,还有 1741,
1750(第二卷的日期是 1749),1770 以及 1790 年本.据说 1750 年
版本是由蒙蒂克拉(Montucla)订正过的,但他不愿署名.最早注明
这些订正的是 1790 年本,但编辑仍只注为 M * * * 先生订正.蒙
蒂克拉删掉了旧版中确属错误的大部分,增添了些历史注记.可
惜由于他过于谨慎而未削除许多琐屑的实验和自明之理.1708 年
出现了原版的一个英译本.我相信它接连出版过四次,最后一次
是 1790 年的都柏林版.赫顿(C. Hutton)翻译了蒙蒂克拉订正的
1790 年本,发行于 1803,1814 与 1840 年(合订本).我参考的就是
1803 年的和 1840 年的两种版本.

我将列举一些典型的关于数字的初等问题.它们是近三个世纪来多数趣味数学方面著述的主要内容.这里给出它们,主要是从历史的角度而不是从算术的兴趣考虑的.数学家完全可以跳过这一章而不必看它.

这些问题性质上多数属于戏法或迷惑人的诡辩.我按惯常
的方式处理它们.不过,即使作为戏法,它们也多半是不值一提
的,除非所用的方法很隐晦或者所得结果出人意料.然而我不是
在写戏法,所以不去谈怎样把其中的运算掩饰起来,而将仅仅列
出所用方法的主要的步骤.对于非数学家来说,即使在今天,那
[4] 些结果之中有些仍似乎是令人吃惊的.不过,一旦用数学符号语
言表述出来,秘密就立即被揭穿了.

猜出一个人所想的数

只要知道了一个人所想的数进行某些运算后所得的结果,就能猜出他所想的数,这种办法有无穷多.我只介绍典型的几个

我们必须知道，而且我们必将知道

http://maths352.bokee.com

常用办法.任何熟悉初等代数的人都不难编造类似的戏法.

第一个戏法① (i)要对方把他想好的数乘以3.(ii)问他乘的结果是奇数还是偶数;如果是偶数,要他再用2去除;如果是奇数,要他先加上1然后再用2去除.(iii)要他把第二步所得的数乘以3.(iv)问他再用9除第三步所得的数时商为几?好了.假定回答为 n,那么(v)他所想的数必是 $2n$(若第一步的结果为偶数)或 $2n+1$(若第一步的结果为奇数).

论证是显而易见的.任一偶数可以写成 $2n$,对于它施行上述运算时,逐步所得的结果为:(i)$6n$,这仍是偶数;(ii)$\frac{1}{2}6n=3n$;(iii)$3\times 3n=9n$;(iv)$\frac{1}{9}9n=n$.任一奇数可以写成 $2n+1$,对它施行上述运算时,逐步所得结果为:(i)$6n+3$,这仍是个奇数;(ii)$\frac{1}{2}(6n+3+1)=3n+2$;(iii)$3(3n+2)=9n+6$;(iv)$\frac{1}{9}(9n+6)=n+$余数.这就说明了上边所给的戏法.

第二个戏法② 要对方把他想好的数逐步进行下列运算:(i)乘以5.(ii)再加上6.(iii)再乘以4.(iv)再加上9.(v)再乘以5.问他所得最后结果是几?把他的答数减去165,然后再用100去除.商就是他所想的数.

理由也很简单.设他想的数为 n.那么上述逐步运算的结果 [5]
是:(i)$5n$;(ii)$5n+6$;(iii)$20n+24$;(iv)$20n+33$;(v)$100n+165$.

第三个戏法③ 要对方把他想好的数依次进行下列运算:(i)随便用什么数 a 去乘它.(ii)随便用什么数 b 去除前一步所得的积.(iii)随便用什么数 c 去乘这个商.(iv)随便用什么数 d 去除第

---

① Bachet, Problèmes, Lyons, 1624,问题1,p.53.

② 巴协给出了一个类似的戏法.问题Ⅳ,p.74.

③ 巴协,问题Ⅴ,p.80.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

三步所得的积.(v)用原先所想的数除最后的商.(vi)再加上原先所想的数.问他所得的和是多少? a, b, c, d 各是多少? 于是,从这个和里减去 ac/bd,剩下的就是他所想的数.

理由是:如果他想的数是 n,那么前四步运算的结果是 nac/bd;第五步所得为 ac/bd;第六步最后得到的是 $n+ac/bd$.而 ac/bd 是知道的,所以减去它就得到 n.显然,a, b, c, d 取什么数都行(自然 b, d 都不能取为零).例如,$a=12$, $b=4$, $c=7$, $d=3$,只要从第六步的结果里减去 7 就是了.

第四个戏法① 要某人想好一个小于 90 的数,然后逐步进行下列运算:(i)乘以 10,再加上随便一个小于 10 的数 a.(ii)用 3 除第一步的结果,说出余数,譬如 b.(iii)将第二步所得的商乘以 10,再加上随便一个小于 10 的数 c.(iv)用 3 除第三步的结果,说出余数(譬如 d)以及商的从右边数第三位数字.假定他说是 e.于是由已知的数 a, b, c, d, e,立即可以确定他所想的数.具体地说,若该数为 $9x+y$,其中 $x\leqslant 9$, $y\leqslant 8$.且 r 为用 9 除 $a-b+3(c-d)$所剩的余数,则 $x=e$, $y=9-r$.

[6] 证明并不难.设所想的数为 $9x+y$.第一步给出 $90x+10y+a$.令 $y+a=3n+b$,则第二步所得的商是 $30x+3y+n$.第三步给出 $300x+30y+10n+c$.令 $n+c=3m+d$,则第四步所得的商是 $100x+10y+3n+m$,我把它记为 Q.由于 $y\leqslant 8$ 且 $a\leqslant 9$ 而知 $n\leqslant 5$;又由 $n\leqslant 5$ 及 $c\leqslant 9$ 而知 $m\leqslant 4$,故 $10y+3n+m\leqslant 99$.所以 Q 里的第三个数字,即,百位数,必是 x.

再者,由等式 $y+a=3n+b$ 及 $n+c=3m+d$ 而得 $9m-y=a-b+3(c-d)$.所以,若用 9 除 $a-b+3(c-d)$时的余数为 r,则 $y=9-r$.(只要使 r 为正数,这总是对的;如果 $a-b+$

① Educational Times, London, May 1, 1895, Vol. XLVIII, p.234. 据说这个例子是麦克斯韦(J.C.Maxwell)在他童年时编的.值得注意的是它与前述几个简单的巴协问题的差别是多么大.

我们必须知道，而且我们必将知道

$3(c-d)$是负数，这时 y 就是 r 的绝对值．也可以取适当的 a 与 c 的值使这种情况不发生．）于是 x 和 y 都知道了，所以他想的数 $9x+y$ 也就知道了．

第五个戏法① 要某人想好一个小于 60 的数．请他实行以下运算：(i)用 3 除它，说出余数．记为 a．(ii)用 4 除它，说出余数．记为 b．(iii)用 5 除它，说出余数．记为 c．于是，他所想的数就是用 60 除 $40a+45b+36c$ 时的余数．

这个玩法可予以推广，所想的数随便有多大都行．设 a'，b'，c'，…为一组互质的数，p 是它们的乘积．令 n 为任一小于 p 的数，a，b，c，…是分别用 a'，b'，c'，…去除 n 时所剩的余数．找一个数 A，它是积 $b'c'd'\cdots$ 的倍数且比 a' 的某个倍数大 1．再找一个数 B，它是积 $a'c'd'\cdots$ 的倍数且比 b' 的某个倍数大 1．相仿地再找一些数 C，D，…．数论里有计算 A，B，C，…的一定的办法．不过，一般地说，如果 a'，b'，c'，…都很小，那么相应的 A，B，C，…可以由观察而得．我来证明 n 等于用 p 除 $Aa+$ [7]
$Bb+Cc+\cdots$ 时的余数．

令 $N=Aa+Bb+Cc+\cdots$，$M(X)$表示 x 的某个倍数．既然 $A=M(a')+1$，所以 $Aa=M(a')+a$．因此，用 a' 除 N 中第一项（即 Aa）时的余数是 a．又因 B 是 $a'c'd'\cdots$ 的倍数，故 Bb 可被 a' 整除．同理，Cc，Dd，…皆可被 a' 整除．如是，N 中各项除第一项外皆可被 a' 整除．所以，当用 a' 除 N 时，余数为 a．因此

$$N-n=M(a').$$

同理

$$N-n=M(b'),$$

$$N-n=M(c'),$$

$$\cdots\cdots$$

可是，a'，b'，c'，…是互质的，所以

---

① 巴协，问题Ⅵ，p.84：巴协在 p87 上增加了关于这个问题的早期历史的一个注记．

我们必须知道，而且我们必将知道

http://maths352.bokee.com



$$N-n=M(a'b'c'\cdots)=M(p),$$

即
$$N=M(p)+n.$$

今所想的 n 是小于 p 的；故若用 p 去除 N，余数必为 n.

巴协所给的戏法相当于 $a'=3, b'=4, c'=5, p=60, A=40, B=45, C=36$. 如果限制所想的数为小于 420 的数，则可取 $a'=3, b'=4, c'=5, d'=7, p=420, A=280, B=105, C=336, D=120$.

什么都不问、早已知结论

请人心想一个数，然后让他进行一系列指定的运算. 什么都不用问他，就可以指出运算的结果. 所有此类游戏本质上都是适当安排一些运算，使所想的那个数和最后的结果没有关系.

例 1① 请某人心里想好一个数. 设它是 n. 你自己随便想定几个数，譬如说 a, b, c. 然后让他(i)用 a 乘他想的数；
[8] (ii)再加上 b；(iii)再用 c 除第二步所得的和；(iv)再减去原数的 c 分之 a 倍. 他得的最后结果必是 b/c. 这是因为前三步运算的结果是 $(na+b)/c$. 第四步要减去 na/c，剩下的 b/c 是你自己早已知道的. 例如，取 $a=6$, $b=12$, $c=4$, 则 $a/c=3/2$，最后的结果是 3.

例 2② 请一个人 A 随便拿几个筹码. 假定他拿的是 n 个. (i)再请另一位 B 拿 p 倍于 A 的那么多，p 是你自己任意想定的一个数. (ii)请 A 把他的 q 个筹码给 B，q 也是你自己任意想定的数. (iii)然后，请 B 把他的筹码转给 A 一些，其数目为 A 现有筹码的 p 倍. 这时，留在 B 手里的筹码必是 $q(p+1)$ 个，这个数目你是知道的. 这个游戏可以用口说的方法（不一定非借用筹码不可）或随便什么办法去玩.

---

① 巴协，问题Ⅶ，p.102.

② 巴协，问题Ⅻ，p.123. 巴协把这个游戏玩得更一般化，但不大好玩.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

道理如下：第二步的结果是 B 手中有 $pn+q$ 个筹码而 A 手中有 $n-q$ 个筹码. 在第三步中，B 转给 A 的筹码的个数是 $p(n-q)$，所以 B 自己手中剩下的筹码的个数是 $(pn+q)-p(n-q)$，即 $q(p+1)$.

例如，设 A 原有任何几个筹码. 假定你取 p 为 2，q 为 3. 首先你要求 B 拿的筹码是 A 的二倍. 然后你又要求 A 给 B 三个筹码. 最后你又要求 B 给 A 一些筹码，其数目为 A 现有筹码的二倍. 这时你知道 B 手中剩下 $3(2+1)$ 即 9 个筹码.

这个游戏也可以只和一个人玩，只要用他的右手代表 A，左手代表 B 就是了. 下边的有些游戏也是这样.

例 3 请某人按顺序完成以下运算：(i)取任一个三位数，要
它的首位和末位的差大于 1；(ii)交换首位和末位数字而构成另 [9]
一个数；(iii)求此两个三位数的差；(iv)颠倒这个差的各位数字的次序，又构成一个新的数；(v)将第三步所得的数与第四步所得的数加到一起. 这时所得的和必是 1089.

下边通过一个实例说明其中的道理：

(i)	732	$100a+10b+c$
(ii)	$\underline{237}$	$\underline{100c+10b+a}$
(iii)	495	$100(a-c-1)+90+(10+c-a)$
(iv)	$\underline{594}$	$\underline{100(10+c-a)+90+(a-c-1)}$
(v)	$\underline{1089}$	$\underline{900+180+9}$

以上运算的结果完全取决于所用记数制的基数. 若基数是 r，则结果是 $(r-1)(r+1)^2$. 如 $r=10$，则结果是 9×11^2，即 1089. 可以用超过 999 的数做类似的游戏.

例 4 下述涉及负数的游戏是 N·安宁(Norman Anning)提出来的. 请某人按顺序完成以下运算：(i)写下任一个大于 1 的数(不必是整数)；(ii)求其倒数(就像由 2 得到 1/2，或由 1/2 得到 2 那样)；(iii)减去 1；(iv)再求倒数；(v)从 1 里减之，(vi)再求倒数；(vii)加上原先写下的数. 这时所得结果一定是 1.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

例如，取数 3/2，依次得(i)3/2，(ii)2/3，(iii)1/3，(iv)3，(v) −2，(vi) −1/2，(vii)1.

下边的解析说明实质且表明最后的结果与最初写下的数是无关的：

(i)a，(ii)$1/a$，(iii)$(a-1)/a$，(iv)$a/(a-1)$，

[10] (v)$1/(1-a)$，(vi)$1-a$，(vii)1；

或者借用 θ① $=\sec^{-1}\sqrt{a}$ 作更简洁的表述：

(i)$\sec^2\theta$，(ii)$\cos^2\theta$，(iii)$\sin^2\theta$，(iv)$\operatorname{cosec}^2\theta$，

(v)$-\cot^2\theta$，(vi)$-\tan^2\theta$，(vii)1.

把第(vii)步换成"再从 1 里减去第(vi)步的结果"也许更自然些.那样，最后得到的就是最初写下的数.

在叙述进一步的游戏之前，值得提一下的是，现在可以买到由拉博斯涅(A. Labosne)审查、简化并增补的巴协的书②第 5 版，其中载有巴协的一帧漂亮的肖像和一篇简短的传记.可以料想他写这本书是为了熏陶他的七个儿子，不过，事实上该书初次出版早在他结婚之前.

涉及两个数的游戏

有一类涉及两个数的游戏，以下给出两个例子.

例 1③ 任取两个数，一奇、一偶.请某甲任选其中的一个，另一个留给某乙.游戏是要猜出某甲所选的是奇数还是偶数.请甲用 2 或任何偶数乘他所选的数，乙用 3 或任何奇数乘留给他的数.再请他们把两人的数加到一起，并把结果告诉你.如果这

---

① 关于这个 θ 角的涵义，见 H.S.M. Coxeter, Non-Euclidean Geometry, Toronto, 1968, p.105.

② C.G. Bachet, *Problèmes plaisants et délectables*. A. Blanohard, Paris, 1959.

③ 巴协，问题Ⅸ，p.107.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

结果是个偶数，那么甲原先选的必是奇数；如果这结果是个奇数，那么甲原先选的必是偶数．理由是明显的．

例 2① 请某人想好两个正数（可以相等且不必是整数）并
依次完成以下运算：(i)将第二个数加 1，然后用第一个数去除而 [11]
得到第三个数．(ii)将第三个数加 1，然后用第二个数去除而得到第四个数……(v)将第六个数加 1，然后用第五数去除而得到第七个数．于是，这第六个数和第七个数分别等于第一个数和第二个数．这样做下去所得的序列是周期的，每个周期包括五个数．（令 a，b 分别表示第一个数和第二个数，很容易证明这个论断．）

取决于记数制的游戏

寻求两个或多个数的许多办法都依赖于这件事实：在算术中一个整数是用一系列数字表示的，其中每位数字表示该数字与十的几次幂的乘积，而整个数就等于这些乘积的和．例如，2017 表示$(2\times10^3)+(0\times10^2)+(1\times10)+7$，即，2 表示两千（2 与 10^3 的乘积），0 表示零个百，1 表示一个十（1 与 10 的乘积），7 表示七个单位．如此，每位数字有一个位上值．通过下列三个例子可以了解记数制在数字游戏中的应用．

例 1② 一个常见的戏法是请听众中一个孩子掷两个骰

---

① R. C. Lyness, Mathematical Gazette, 1942, Vol. XXVI, p. 42 (Note 1581); 1945, Vol. XXIX, p.231 (Note 1847)．关于有关的游戏"弗里兹(Frieze)图案"，请看 H. S. M. Coxeter, Acta Arithmetica, 1971, Vol. XVIII, pp.297—310．

② 类似的游戏见于巴协，问题Ⅺ，p.117；奥特雷德(Oughtred)或利克(Leake)：Mathematical Recreations，通常认为是前者的著作，London，1653，问题 XXXIV；Ozanam, part Ⅰ, chapter Ⅹ．Mathematical Recreations 可能是利克编纂的，但此书通常列于奥特雷德(W. Oughtred)的名下．我将在下边介绍这种游戏，它的本源是 1626 年出版的 J·勒雷雄的同类的著作，或谓为范埃滕(H. van Etten)的著作．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

子，或者从一个匣子里任意摸出一枚骨牌，每枚骨牌的一端上都刻着一些点．然后叫这孩子记住这两个点数，并且把其中任一个乘以 5，再加上 7，再乘以 2，最后再加上两个数中的另一个．魔术师从这孩子最后得到的数里减去 14 而得到一个两位数，这两个数字就是原先那两个骰子或两枚骨牌上的点数．

〔12〕 道理：假定这孩子得到的点数是 a 与 b．骰子也好、骨牌也好，这些点数都是小于 10 的．逐步运算所得结果依次为：(i)$5a$；(ii)$5a+7$；(iii)$10a+14$；(iv)$10a+14+b$．所以，当你从最后的结果里减去 14 时，必得一个这样的两位数，它的两个数位上的数字正是原先所得的两个点数．如果想要把这种游戏做得更神秘些，还可以用别的计数制编成类似的游戏．

例 2① 相仿地，如果任意取三个数：a，b，c，每个都小于 10．用下述办法可以找出它们．(i)取其中的一个数，譬如说 a，乘以 2；(ii)然后加 3；(iii)再乘以 5，然后再加 7；(iv)将此和数与第二个数 b 相加；(v)然后乘以 2；(vi)再加 3；(vii)再乘以 5，然后与第三个数 c 相加．这时得到的结果是 $100a+10b+c+235$．因此，如果知道最后所得的数，那么只要减去 235，得到的差必是那样一个三位数，它的三个数位上的数码正是原先所取的三个个位数．

例 3② 下边猜出一个人的年龄的游戏和前两例子是属于同一类型的．叫他想好一个数（最好不超过 10）；(i)平方之；(ii)减 1；(iii)用原先想的数乘此结果；(iv)再乘以 3；(v)加上他的年龄；(vi)说出得数的各个数位上的数码的和．这个和与他的年龄的数码和是相同的．所以你可以猜出他的年龄，不过，可能差一个九的倍数．

这个游戏的代数证明是显然的．设年龄为 a，他想的数是

① 巴协在他的问题Ⅻ(p.117)里有类似的阐述．

② 据希思(R.V.Heath)．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

b. 逐步运算所得为(i)b^2;(ii)b^2-1; (iii)$b(b^2-1)$; (iv)$3b(b^2-1)$; (v)$a+3b(b^2-1)$;(vi)a 的数码和,因为 $3b(b^2-1)$恒为 9 的倍数.

其他例子[①] 另一个较困难的此类问题是求所有那样的数,它是它的逆序数的整数倍.例如在四位数中,8712 = 4 × [13] 2178, 9801 = 9 × 1089,这两个数就具有此种性质.

还有,可以求两个那样的数,它们各自的逆序的乘积恰好是它们的乘积的逆序.例如

$$312\times221=68\,952,\ 213\times122=25\,986.$$

数 698 896 有不平常的性质.它是一个完全平方数,等于它的逆序数,并且是一个偶位数.

仅有四个数具有这样的性质,它等于它的各位数码的立方和:[②]$153=1^3+5^3+3^3$,$370=3^3+7^3+0^3$,$371=3^3+7^3+1^3$,$407=4^3+0^3+7^3$.

1/7 的十进位循环小数的性质也是出名的.

特罗伊茨基(Troitsky)曾经证明[③]:在小于一百万的数中,只有 142857 和 285714 这两个数,当我们把它们的首位移到末位时所得结果是原来的整数倍.

十进制数的其他有趣问题

我在此介绍几个其他的问题,它们似乎不为多数趣味数学编纂者所知.

问题 1 叫某人任意想一个三位数,其第一位数码不要和

---

① L'Intermédiaire des Mathématiques, Paris, Vol. XV, 1908, pp. 228, 278; Vol. XVI, 1909, p.34; Vol. XIX,1912,p.128. M.Kraïtchik, La Mathématiques des Jeux, Brussels, 1930, pp.55, 59.

② Sphinx (Brussels), 1937, pp. 72,87.

③ L'Echiquier, 1930, p.663.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第三位数码一样;颠倒这三个数码的次序而构成另一个数;将此数与原先的数相减;问他得数的末一位是几,那么你就可以指出他的整个得数是什么.

秘密在于:若所想的数是 $100a + 10b + c$,则颠倒数码的次序而构成的数是 $100c + 10b + a$.这两个数的差是 $(100a + c) - (100c + a)$,即,$99(a - c)$.但 $a - c$ 不大于 9,所以这个差只能是 99,198,297,396,495,594,693,792 或 891.在任一情况下,中间的数码都是 9,并且前一个数码总是等于 9 减去末一位数码.因此,只要知道了末一位数码,整个差数就肯定了.

问题 2 这个问题和前一个有些类似,其提法如下:(i)任取
[14] 一数;(ii)颠倒数码的次序;(iii)求(i)与(ii)中两个数的差;(iv)用任何数乘此差;(v)抹掉除了零之外的任一数码;(vi)读出留下的数码.你知道被抹掉的数码是什么吗?欲知答案,可先把留下的数码加起来,再看用什么数码与这个和数相加结果是 9 的一个整倍数.这个数码就是被抹掉的数码.

道理是明显的.第(iv)步运算的结果是 9 的一个整倍数,而任一 9 的整倍数的数码和仍是 9 的一个整倍数.此问题与前一问题都是许多此类问题的典型.

问题 3 如果给一本书逐页编码总共需要 n 个数码,那么这本书共有几页?例如,$n = 3001$.

显然,前 999 页需要用 $9 + 90 \times 2 + 900 \times 3$ 即 2889 个数码.但另外还用了 $3001 - 2889 = 112$ 个数码,它们恰够再标记 $112 \div 4 = 28$ 页.所以这本书共有 $999 + 28 = 1027$ 页.

问题 4 从 1 开始挨个儿往后写正整数,问第 n 个数码你应该写什么?例如 $n = 500\,000$?

从 1 写到 99 999 共需写 $9 + 180 + 2\,700 + 36\,000 + 450\,000$ 即488 889个数码.接下去从 100 000 开始还应写 $500\,000 - 488\,889$ 即 11 111 个数码.这些数码足够写 1 851 个六位数,因为

我们必须知道，而且我们必将知道

http://maths352.bokee.com

11 111＝6×1 851＋5. 剩下的 5 个数码该去写第99 999＋1 851＋1 个数即 101 851 的前 5 个数码. 所以你最后写的是 5.

拼凑问题 还有许多拼凑性的问题如下：用十个数码 9,8,7,6,5,4,3,2,1,0 作成一些数，要它们的和等于 1；每个数码只许用一次，且可用分数符号. 又，用这十个数码作成一些数，要它们的和等于 100. 又，用九个数码作成一些数，要它们的和等于 100. 此类问题要多少个就能编多少个，它们的解答没有什么数学技巧可言.

四个数码的问题 我想下边的问题更为有趣. 用数码 1,2,3,4 表达由 1 开始依次相邻的正整数，在每个数的表达式里都要用上这四个数码而且每个数码只许用一次. 采用十进制记数 [15] 法，可以运用代数和、相乘以及正整数幂. 问你最多能做到哪个数. 我们能做到 88. 如果还允许用开平方与求阶乘符号(需要时可重复使用有限次)，那么我们能做到 264；如果还允许用负整数作指数，那么能做到 276；如果再允许用分数作指数，那么能做到 312.

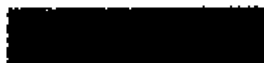
还可以提许多类似的问题. 例如，从 1,2,3,4,5 里随便取用哪四个数. 又如，要把 1,2,3,4,5 都用上而且每个表达式里只许各用一次，我曾做到 3 832 或 4 282，看是否允许使用负数与分数作指数而定.

四个 4 的问题 另一个传统的游戏是，借助于通常的算术和代数运算符号与四个数码“4”，去表达由 1 开始依次相邻的正整数，问你最多能做到哪个数. 这要看“通常的……运算符号”包括些什么而定. 若(i)它指十进制(如 44 之类的数)、十进小数、括号、加号、减号、乘号与除号，则可表达直到 22 在内的每个数①. 若(ii)还允许用开平方号(需要时可重复使用有限多次)，

① 例如，$22=(4+4)/(.\dot{4})+4$.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



则可前进到30；不过要注意，虽然有了开平方号则只要拿一个4开平方就得到2，却不能因此就说2可以表示为4的开平方.若(iii)此外还允许用阶乘号，那么可以表示从1到112的每一个数①.最后.若(iv)准许用一个“4”或几个“4”表示的整数作为指数，并且准许无限多次地使用开平方号，则可做到156；再者，若(v)许可使用整数作指数且可采用次阶乘运算②，则可达到877.这些有趣的问题是一类相仿问题的典型.譬如，在条件(v)之下且不用指数，则用四个“1”可进行到34，用四个“2”可到36，用四
[16] 个“3”可到46，用四个“5”可到36，用四个“6”可到30，用四个“7”可到25，用四个“8”可到36，用四个“9”可到130.例如，哈吉(T. Haji)曾指出 $67=\sqrt{9!/(9\times 9)+9}$.

一组有编号物品的问题

任一连续标号的物品的集合皆可用以对取决于数的初等性质的问题作简易的例释.作为例子，我将说明几个熟知的游戏，其中头两个通常用一块手表作表演，后四个可用一副纸牌作为示范.

例1 ③ 这些例子的第一个是关于表盘上的钟点标记的.在这个游戏里，让某人心里想好一个钟点，譬如 m，然后再让他指点另一个钟点，譬如 n.这时如果他从所指点的钟点开始沿反时针转动方向依次指点表盘上的钟点，同时数数 m，$m+1$，…，则当数到 $n+12$ 时，他指点的必是他开始所想的钟点.例如，如果他想的是Ⅴ而指的是Ⅸ，那么当他一边往

---

① 例如，$99=4\times 4!+\sqrt{4/(.\dot{4})}$.

② n 的次阶乘等于 $n!(1-1/1!+1/2!-1/3!+\cdots\pm 1/n!)$.关于把次阶乘用于四个“4”的问题，请参看 Mathematical Gazette，May 1912.

③ 巴协，问题 XX，P.155；Oughtred 或 Leake，Mathematical Recreations，London，1653，p.28.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

回指点Ⅸ，Ⅷ，Ⅶ，Ⅵ，…一边数5，6，7，8，…，数到21时正好指到Ⅴ上.

道理是明显的，因为他只要沿逆时针方向数 $n-m$ 步就到达 m 点了.他实际数了 $n+12-m$ 步.这多出的12步只不过多转一圈，最后仍然要停在 m 点上.以上是就 n 大于 m 的情况而言.如果 n 小于 m，为了使游戏照样能够玩，先在 n 上加一个12就是必要的了，这时 $n+12-m$ 仍是一个正数.所以，不论哪种情况，游戏都一样进行.

例2　下边是另一个熟知的表盘问题.如果让某人心中想 [17]
好一个钟点之后，从表盘上的Ⅶ开始沿逆时针方向指点Ⅵ，Ⅴ，…，同时从他所想的点数往下数数(譬如，他想好的是Ⅹ，那么就从11开始往下数)，当他数到20时，他指的就是他所想的钟点了.

因为如果他想好的是第 n 点钟，则他第8下指点的是Ⅻ而口里数的是 $n+8$.当他数到 $n+p$ 时指点的就是 $20-p$ 点钟.因此，取 $p=20-n$，则当他数到20时，指的正是 n 点钟.自然，前七下指的钟点都是无关紧要的.显然，我们可以让他从Ⅷ点处开始而数到21，或者从Ⅸ点处开始而数到22，……最后指点的都是他所想好的钟点.

例3　下边是另一个简单的例子.把一副 n 张的牌摞起来.取上边的 m 张交给某人，让他从中认定一张(不要说出来)并且记住是从顶上数第几张.假定是第 x 张.把牌拿回来，颠倒这 m 张的次序，放在其余 $n-m$ 张的上边.再从最下边任取 y 张($y<n-m$)放到最上边.这时他所认定的牌已经是从顶上数第 $y+m-x+1$ 张了.把牌再交给他，让他从上往下数，第一张算是第 $x+1$ 张，第二张算是第 $x+2$ 张，……当他数到第 $y+m+1$ 张时，你可以指出，它就是他所认定的牌.每次玩时，y 与 m 都可以任意改变.在算术方面不熟练的人不会马上觉察出这里边的奥妙.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

例 4[①] 取牌一张放在桌上，看它是几点，再从同一副牌里取一些牌摞上去，摞上的张数和该点数之和为十二. 例如，若首
[18] 先放在桌上的是梅花五，那么就摞上去七张. K，Q，J 可任意赋值，通常可以都当作十点. 然后再另放一张牌，如法往上摞，于是又成一摞. 继续这样做，直到不够再摞为止. 假定一共得 p 摞，而手中剩下 r 张. 问各摞最下边的那一张的点数之和为多少? 答：$13(p-4)+r$.

因为，若某一摞最下边那一张上的点数为 x，则该摞牌为 $13-x$ 张. 每一摞都是这样. 各摞张数的和加上手中剩的张数应该等于一副牌的总张数 52. 所以

$$(13-x_1)+(13-x_2)+\cdots+(13-x_p)+r=52,$$
$$13p-(x_1+x_2+\cdots+x_p)+r=52,$$
$$\therefore \quad x_1+x_2+\cdots+x_p=13p-52+r$$
$$=13(p-4)+r.$$

一般地，若一副牌共有 n 张，每摞的底张点数与摞上去的张数之和为 m，则各摞底张点数之和为 $(m+1)p+r-n$. 在去掉一部分之后剩下的一副牌里，如 $n=32$，则取 $m=15$ 比较方便.

例 5 容易看出，截牌是永远不会改变各张牌的相对次序的，只要把最上边的牌看成是紧接着最下边那一张牌. 这个事实被应用于下边的游戏中[②]. 取牌一副，把它们一张一张正面向上摆到桌子上. 当你往下放的时候，一边呼一、二、三、……，同时心里暗暗记住第一张是什么牌. 让另一个人随便认定一张，你记住它的呼号。把牌顺次翻过去收成一摞，任意截几次(不要洗). 欲知他认定的是哪一张. 你可以一张一张往后倒，一旦发现你暗记的第一张牌，心中就暗暗从一

① 巴协，问题 XVII，p.138 给出了此问题的一个特例.

② 巴协，问题 XIX，p.152.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

开始数，数到你记住的呼号，出现的就是他认定的那一张了. [19] 当然，如果在没有数到呼号之前，牌已倒完了，就应该接下去从头倒.

例 6 这是此类问题的又一简例. 把带人的牌都挑出去. 把剩下的 40 张牌正面向上分别把同一花色按点数顺次排成一行. 第一行从一点开始：1，2，…，10；第二行从十点开始：10，1，2，…，9；第三行从九点开始：9，10，1，…，8；第四行从八点开始：8，9，10，1，…，7. 然后把第一行第一张正面向上拿起来放到第二行第一张的下边，再把这两张一齐拿起来放到第三行第一张的下边，再把这三张一齐拿起来放到第四行第一张的下边. 把这一摞四张一齐翻成面向下. 然后把第二列的四张牌同样摞起来、翻过去，并把它们放到第一摞的下边. 继续这样做下去，直到所有的牌都摞到一起. 请某人任意说他要一张什么牌. 如果他要的点数是 n 而花色属于第一行，那么从一整摞的最上一张往下数第 $4n$ 张就是他要的牌. 如果他要的牌的花色属于第二行，那就是第 $4n+3$ 张. 如果他要的牌的花色属于第三行，那就是第 $4n+6$ 张. 如果他要的牌的花色属于第四行，那就是第 $4n+9$ 张. 必要时可循环数下去，一定能挑出他要的牌. 这个游戏不难变换成别的面貌，也可以玩整副 52 张牌. 解说是明显的，从略.

算式补码

以下我介绍一类问题，它们都是要求补上算式中被抹掉的数码. 这些问题有些很容易，有些却是困难的. 近年来此类练习很引人注意. 兹给出三类算式补码的例子.

A 类 一类补码问题的解决要借助于众所周知的一些命题：每个数

$$a+10b+10^2c+10^3d+\cdots$$

都和某些表达式中的任一个相等，例如

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$M(9)+a+b+c+d+\cdots$,

[20] $M(11)+a-b+c-d+\cdots$,

$M(33)+(a+10b)+(c+10d)+(e+10f)+\cdots$,

$M(101)+(a+10b)-(c+10d)+(e+10f)-\cdots$,

$M(m)+(a+10b+10^2c)+(d+10e+10^2f)+\cdots$,

$M(n)+(a+10b+10^2c)-(d+10e+10^2f)+\cdots$.

这里倒数第二行中的 m 可取值 27,37 或 111,末一行中的 n 可取值 7,11,13,77,91 或 143.

借助于此类命题的例子并不希奇.下边是四个容易的例子.

(i) 417 与·1···的乘积是 9···057,这里每个圆点表示一个丢失了的数码.求这些数码.

令 a, b, c, d 分别表示乘数中从左到右四个丢失的数码.按相反的次序进行乘法运算的步骤,即相继发现 $d=1$, $c=2$, $b=9$. 又因为乘积有 7 位,故 $a=2$.所以乘积是 9 141 057.

(ii) 七位数 70··34·可被 792 整除.每个圆点表示一个丢失了的数码.求这些数码.

由于 $792=8\times9\times11$,不难证明这个七位数应该是 7 054 344.

(iii) 五位数 4·18·可被 101 整除.求丢失的数码①.

用 x 与 y 表示从右到左两个丢失的数码.引用关于 101 的上述命题且注意每个未知数码都不大于 9,为简便计,令 $y=10-z$,则由命题中的等式得出 $z=1$, $x=7$, $y=9$.所以此五位数是 49 187.

(iv) 四位数·8··可被 1 287 整除.求丢失的数码②.

用 x, y, z 表从右到左丢失的数码.注意 $1\,287=9\times11\times13$.引用上述命题中适当的等式并注意这些未知数都不超过 9.可得 $x=1$、$y=6$、$z=3$.所以此数为 3 861.

---

① P. Delens, Problèmes d'Arithmétique amusante, Paris, 1914, p.55.

② 见前注,p.57.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

(v) 一个稍难的例子.已知 6·80·8··51 可被 73 整除,也可被 137 整除.求丢失的数码①. [21]

所给条件足够确定此数.答案是 6 780 187 951.

B 类 下边的例子说明另一类同时也是较困难的一类补码问题.它们的解决包含着分析的技巧,但归纳不出法则来.

(i) 从一个简单的例子开始,据说此例源于印度.有一个六位数恰被另一个三位数除尽,商也是三位数②.在演算此除法的立式里,大部分数码被擦掉了.附式中每个圆点表示被擦掉的一个数码.问题是要求补出它们来.

```
...)......(...
    .0..
    ----
     ....
     .50.
     ----
      ...
      .4.
      ---
```

解此问题没有什么困难.答案:除数为 215,商为 573.这是唯一的解答.

(ii) 我再给出一个比较困难的例子,它是代尔夫特(Delft)的舒(H.Schuh)教授在 1921 年提出的.有一个七位整数被一个六位整数除.商的整数部分是一个两位数,小数部分是一个十位数,它的末九位构成一个循环节.这个除法运算的立式如下,其中在循环节上标志着一条横线.问题仍是要求恢复擦掉的数码③.这个问题是惊人的,它的数码全被擦掉了. [22]

---

① 见前注,p.60.

② American Mathematical Monthly, 1921, Vol. XXVIII. p.37.

③ 见前注,1922,Vol. XXIX, p.211.

我们必须知道，而且我们必将知道

http://maths352.bokee.com


```
                        ______________
......)  .......(  ..............
         ......
         ______
         .......
          ......
          _______
          .......
          .......
          ________
            .......
             ......
             _______
             .......
             .......
             ________
               .......
               .......
               ________
                 .......
                 .......
                 ________
                   .......
                   .......
                   ________
                          ......
                          ......
                          _______
                          ......
```

答案是：除数为 667334， 被除数为 7752341， 商为 11.6168830001.

下边是另外三个算式补码问题①.解答是冗长的，包含着经

① 这三个问题都是贝维克(W.E.H.Berwick)给出的."7"的问题见于 School World, July and October, 1906, Vol. Ⅷ. pp.280—320;"4"的问题见于 Mathematical Gazette, 1920, Vol. Ⅹ, pp.43,359—360;"5"的问题见于同卷 p.361 及 Vol. Ⅺ, p.8.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



验性很强的工作. [23]

(iii) 这些贝维克问题的第一个是:在下列一个除法运算的立式里,除了七个"7"以外,别的数码都被擦掉了.每个被擦掉的数码都可能是 1,2,3,4,5,6,7,8,9 或(除了每个数的最左边的一个数位)0.注意这里每一步减法运算中相减的两个数的位数都是相同的.问题要求补上所有的数而恢复原来的立式.解答是唯一的,除数是 125 473,商是 58 781.

```
....7.)..7.......(..7..
       ......
       ------
       .....7.
       .......
       -------
           .7....
           .7....
           -------
           .......
           ....7..
           -------
               ......
               ......
               ------
```

(iv) 第二个问题是相仿的,要求补上下列除法运算立式中所有被擦掉的数码.式中留下了所有的"4".

```
...)......4(.4..
        ...
        ---
        ..4.
        ....
        ----
          ....
           .4.
           ---
```


我们必须知道，而且我们必将知道



```
 . . . .
 . . . .
 ———
```

[24]

这个问题有四组解，它们的除数分别是 846，848，943，949，相应的商是 1 419，1 418，1 418，1 416.

如果把问题的提法改为(用五个“4”)：

```
. . . ) . . . . . . 4 ( . 4 . .
        . . .
        ———
        . . 4 .
        . . . 4
        ————
          . . . .
           . 4 .
          ————
           . . . .
           . . . .
           ————
```

那就只有一组解了. 有人认为这样提法较好.

(v) 这些贝维克问题的最后一个是要恢复下列除法运算的立式，其中除了留下五个“5”以外，别的数码都被擦掉了.

```
. . . . ) . 55 . . 5 . ( . 5 .
          . . 5 . .
          —————
           . . . . .
           . . . . .
           —————
             . . . .
             . . . .
             ————
```

此问题仅有一组解：除数是 3 926，商是 652.

C 类 第三类数码问题是求一些字母所代表的数码. 两个

[25] 例子够了.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



(i) 一个非常简单的例子：*bc* 乘 *bc* 的结果是 *abc*，字母 *a*，*b*，*c* 表示的是一些什么数码？稍微想一想就知道 *bc* 表示的是 25，因而 *a* 必为 6.

(ii) 另一个例子. 要求找出下列算式中字母代表的数码①：

```
ab)cdeeb(bfb
    ceb
    ---
    gge
    gch
    ---
     ceb
     ceb
     ---
```

这么分析可以找到一组解：因为 *b* 乘 *b* 的结果须是末位仍为 *b* 的数，所以 *b* 只能是 1，5 或 6. 又因为 *ab* 与 *b* 的积须是一个三位数，所以 *b* 不可能是 1. *e* 减 *h* 的结果仍是 *e*，故 $h=0$，因而若 $b=5$ 则 f 为偶数，若 $b=6$ 则 $f=5$. 再者，*g* 减 *c* 等于 *c*，故 $g=2c$，因而 *c* 不能大于 4. 由此可推知 *b* 不能等于 6. 再作不几步试探即知原问题为 35 除 19 775.

可以编造具有混合性质的补码问题，它们具有以上各个例子所包含的困难. 还可以采用非十进制去增加问题的复杂性. 但这样做并不增加问题的趣味.

日 历 问 题

我在本书的前几版里引述过的高斯(C. F. Gauss)与泽勒(Zeller)的公式，可用以解决经常遇到的关于日期、星期几、圣诞节等等的各种问题. 下边是两个容易而漂亮的关于格雷戈里(J. [26]

① Strand Magazine, September – October, 1921.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Gregory)日历的问题,其性质有些不同.

第一个有如下述:我相信它是富雷(E. Fourrey)给出的.在1725到1875这一个半世纪中某年的4月22日法国人打了一个胜仗,过了4 382天之后,也是在一个4月22日,他们又赢得了一次胜利.这两个年份的数码之和为40.问这两次战争发生的日期.

要解答这个问题,先注意 $4\ 382 = 12 \times 365 + 2$.所以第二次战争日期与第一次战争日期相隔12年.但这里边只有过两个闰年,所以1800这个年份必在这13个年份之内.于是,可能的答案有1788与1800;1789与1801;…;1800与1812.这13个可能的答案中,只有1796与1808的数码和是40.所以两次战争发生的日期是1796年4月22日[拿破仑(Napoleon)指挥的蒙多维(Mondovi)战役]、1808年4月22日[达武斯特(Davoust)指挥的埃克米尔(Eckmuhl)战役].

第二个问题是:证明每隔一个世纪的第一天或末一天必为星期五.只要知道任何一个指定的日期,据格雷戈里周期是400年(=20 871个星期)这件事实就可得到这一论断.同一个原理也包含在布朗(B. H. Brown)的断言①里:每个月的第13天是星期五要比是星期一、二、三、四、六或者星期日的可能性都大.

中世纪的算术问题

在结束初等问题这一主题之前,我再叙述几个世纪以来几乎在每本数学游戏的书里都出现的一些问题,因此照惯例应该放在这里.

例1 下边是此类趣题的一个代表.一人池边去取水,两个罐子不一般,各容3kg与5kg,要取4kg怎么办?

[27] 这是容易解决的.

① American Mathematical Monthly, 1933, Vol. Ⅺ. p.607.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



例 2[①] 下边是又一个此类问题.三个强盗劫得一瓶香浆,原装满瓶净重 24 盎斯.逃到半路遇见一个瓶商,买了三只空瓶好去分赃.潜至据点坐下量了又量,发现瓶子大小全不适当,标着容量 5,11,13 盎斯.怎样才能分成三份一样?

这种问题可用试着干的办法解决.

例 3[②] 其次也是一个平常的博弈.A,B 两人轮流说数.开始时 A 先说一个不得大于(譬如)6 的数,B 往上加一个不大于 6 的数,接着 A 再往上加一个不大于 6 的数,如此继续下去.谁先得到(譬如)50,谁就算赢.

显然,如果 A 得了 43,那么不论 B 往上加什么数(当然限于不大于 6 的数),下次 A 就赢了.相仿地,如果 A 得了 36,B 就无法阻拦 A 在下一次得 43.依此推下去,关键的数字是算术数列 43,36,29,22,15,8,1;谁先得到其中任何一个谁就必然能赢.

相仿地,如果每次加上的数不许大于 m,n 是赢家争得的数,那么关键数为一个公差为 $m+1$ 的等差数列,它的最小项是用 $m+1$ 除 n 时的余数.

这个游戏也可按另外的形式来玩.譬如把 p 个钱币,p 根火柴,或者别的什么东西放在桌上.规定每位参加者轮流取走不超过 m 个所放的东西.拿走最后一个为赢.显然,关键数是 $m+1$ 的倍数.谁先使桌上剩的钱币为 $m+1$ 的整数倍谁就能取胜.也许这个游戏的更好的玩法是规定取走最后一枚钱币者为输,这时关键数是 $m+1$ 的倍数加 1. [28]

---

① 巴协给出了一些类似的问题,见他的书的附录,问题Ⅲ,p.206;此外,参看 Mathematical Recreations, p.22,奥特雷德或利克给的问题;又,1803 年版中,Vol Ⅰ,p.174,1840 年版,p.79,奥札南所给的问题.更早的例子见于塔尔塔利亚的著作中.又见于 Kraïtchik, p.11; H.S.M. Coxeter and S.L.Greitzer, Geometry Revisited. New York, 1967, pp.89—93.

② 巴协,问题 XXII, p.170.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



另一个变形①是把 p 个筹码摆成一个圆圈，参加游戏的人轮流每次取走至多 m 个相邻的筹码，m 小于 p 而大于 1. 这种游戏如果是两个人玩，开始先取者必输.

这些游戏是简单的，但是如果对原来的玩法加上限制：每个参加者采用同一个加数不许超过（譬如说）三次，要分析清楚就决非容易的事了. 我从未见到什么书刊上有这种推广. 以下就来作详细的讨论.

假定给每位参加者发 18 张牌：三张 6 点，三张 5 点，三张 4 点，三张 3 点，三张 2 点，三张 1 点. 他们轮流出牌. A 先出一张，然后 B 出一张，等等. 谁先出的牌使得桌子上的牌的全部点数之和等于 50 谁就算赢了. 但若那张牌使全部点数之和超过了 50，他就算输了. 这个游戏也可以在纸上写数的办法来玩而不必用牌.

看一个实际过程：A 出 4，记录一个 4；B 出 3，记录 7；A 出 1，记录 8；B 出 6，记录 14；A 出 3，记录 17；B 出 4，记录 21；A 出 4，记录 25；B 出 5，记录 30；A 出 4，记录 34；B 出 4，记录 38；A 出 5，记录 43. 现在 B 能操胜券了，因为只要他出 3，而 A 已经把手中的 4 点牌出完了，如果 A 出点数小于 4 的牌，下次 B 出牌就赢了.

再看一个过程：A,6； B,3； A,1； B,6； A,3； B,4； A,2； B,5； A,1； B,5； A,2； B,5； A,2；B,3. 现在 A 只好出 1，于是接下去 B 出 1 而赢.

这个游戏还有一种稍微不同的玩法. 这种玩法是大家商定在桌上放一定数量的牌，譬如说，一、二、三、四、五、六各 4 张，共 24 张. 每位参加者轮流取牌一张. 每有人取一张牌就计算一次
[29] 大家取走的牌的点数和. 先使点数和等于（譬如说）50 者赢，使点数和不得不大于 50 者输.

假定他们玩的过程如下：A 取一张 6，记一个 6；B 取一张 2，

---

① S. Loyd, Tits-Bits, London, July 17, Aug. 7, 1897.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

累计为 8；A 取一张 5，累计为 13；B 取一张 2，累计为 15；A 取一张 5，累计为 20；B 取一张 2，累计为 22；A 取一张 5，累计为 27；B 取一张 2，累计为 29；A 取一张 5，累计为 34；B 取一张 6，累计为 40；A 取一张 1，累计为 41；B 取一张 4，累计为 45；A 取一张 3，累计为 48；B 现在只好取一张 1，累计为 49；于是 A 取一张 1 而赢.

在这些变动了的玩法里，每位参加者的目标都是设法占住一个关键数字，只要还留有充分多的可用数字，他就要步步保持占住下一个关键数字．游戏中用牌的张数、牌上的点数、争取达到的点数和都可任意约定．达到的点数和愈大，结局愈难预料，也愈难说首先玩的人是否占便宜.

例 4　下边的中古问题更复杂些．假定有三个人 P,Q,R 选取三件东西，分别记为 a,e,i．要弄清谁选的是哪一件①.

往桌上放 24 个筹码．让 P 取一个筹码，Q 取两个筹码，R 取三个筹码．然后，让选 a 的人取和他手中一样多的筹码，让选 e 的人取两倍于他手中那样多的筹码，让选 i 的人取四倍于他手中那样多的筹码．此刻看看桌上还剩几个筹码．把三件东西分给三个人有 6 种不同的方案；对应于每个方案，桌上剩的筹码的数目是各不相同的，它们是 1，2，3，5，6 或 7．巴协将此结果总结为一句便于记忆的话②：

Par fer (1) César (2) jadis (3) devint (5) si grand (6) prince (7).

对应于剩余筹码的每一种数目，有一个双音节字或两个单音节字．例如，余数 5 对应着法文字 devint，它的第一个音节的元音 [30]

① 巴协，问题 XXV，p.187.

② 此句法语意为“昔日恺撒依仗武力而成为了不起的帝王”．但对于这个游戏来说，重要的是这句话的拼写中依次包含的元音字母正好是“a,e；e,a；a,i；e,i；i,a；i,e”这 6 种组合．读者做游戏时记住这 6 种组合的顺序就行了．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

表示 P 选的东西是 e，第二个音节的元音表示 Q 选的东西是 i，于是 R 选的东西自然是剩下的 a 了.

推广 博莱特(M.Bourlet)在对本书第2版的一篇非常恳切的评介①中给出了上述问题的一个很漂亮的推广. 设参加游戏的有 n 个人，$P_0,P_1,P_2,\cdots,P_{n-1}$，每人从一组 n 个物品(例如骨牌或扑克牌)中选取一个. 要想知道各人选的是哪一个.

假定用数字 $0,1,\cdots,n-1$ 而不再用元音字母去区别这些骨牌. 先在桌上放

$$M\geqslant\sum_{h=0}^{n-1}h+\sum_{h=0}^{n-1}n^h h$$

个筹码. 给 P_1 一个筹码，给 P_2 两个筹码，……，一般地，给 P_k k 个筹码，$k=0,1,2,\cdots,n-1$. 然后让选0号骨牌者自取像他手中一样多的筹码，让选 h 号骨牌者自取为他手中的 n^h 倍之多的筹码，例如 P_k 选的是 h 号骨牌，就让他自取 $n^h k$ 个筹码. 于是全体 n 个参加者自取的筹码共为 $N=\sum n^h k$ 个. 你只要看一下桌上还剩下几个筹码，譬如说是 L 个. 那么你立刻可以算出②

$$N=M-L-\sum_{k=0}^{n-1}k=M-L-\frac{1}{2}n(n-1).$$

于是再用 n 除 N，若商为 Q_1，余数为 r_1，则 P_{r_1} 选的是0号牌；再用 n 除 Q_1，余数为 r_2，则 P_{r_2} 选的是1号牌；等等. 换句话说，如果把 N 换算成 n 进制的数，则若从右数第 $h+1$ 位数码为 k 就表明 P_k 选的是第 h 号牌.

照此，在巴协问题里有三个人和三张牌，我们应当给 Q 一个筹码，给 R 两个筹码，而不给 P 筹码. 然后要选0号骨牌(即 a)者自取像他手中一样多的筹码，要选1号骨牌(即 e)者自取为他手中的三倍之多的筹码，要选2号骨牌(即 i)者自取为他

---

① Bulletin des Sciences mathematiques, Paris, 1893, Vol. XVII. pp. 105—107.

② 原著此段含糊，兹予补订.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



手中的九倍之多的筹码.注意原来的筹码的个数而且已经把其 [31]
中的三个给了 Q 与 R,我们就知道了 P、Q 与 R 自取筹码的总数.将此总数除以 3,余数就表明谁选了骨牌 a(余数为 0 表示是 P,余数为 1 表示是 Q,余数为 2 表示是 R);再将此商数除以 3,余数就表明谁选了骨牌 e,第二次的商数表明谁选了骨牌 i.

拓荒问题 另一个普通的问题是拓荒者由前哨向荒原深进的最大进程问题.假定他能够携带 a 天的给养,并允许他在前哨建立仓库而存贮 n 次.答案是,如果他要回家,则最远的进程是

$$\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots+\frac{1}{2n}\right)a$$

天的路程,如果不回家,则最远的进程是

$$\left(1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n-1}\right)a$$

天的路程①.

约瑟夫斯问题 另一个古老的问题是要把一些人安排在一个圆桌周围.从某处数起,每逢第 m 个人就杀掉,然后接下去重新数起,使得最后存活的是预定的几个人.这样的问题很容易用试数的办法解决.

赫格西帕斯(Hegesippus)②说约瑟夫斯(Josephus)就是用一个这种安排救了他的命.据他说,罗马人攻夺乔塔帕特(Jotapat)后,约瑟夫斯和其他 40 个犹太人避难到一个洞穴里.使约瑟夫斯非常反感的是,他发现除了他自己和另一个人之外,其余的都决心殉难以免落入征服者的手中.他不敢太公然表示反对而只
好同意了,但他宣布,这一行动必须有条不紊地进行,并且建议 [32]

① D. Gale, American Mathematical Monthly, 1970. Vol. LXXVII. pp.493—501.

② De Bello Judaico, bk. Ⅲ, chaps. 16—18.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



大家坐成一个圆圈然后点数“一、二、三”，凡是数到三的人就杀掉，直到最后一个人去自杀.他把自己和赫格西帕斯分别排到第16和第31号位置上①.

这个中古时代的问题有一个常见的提法如下.载着15位土耳其人和15位基督徒的一艘轮船遇到了风暴.为了挽救乘客和这条船，必须把乘客的一半扔到海里.于是乘客们被安排站成一个圆圈.从某个人开始点数，每数到9就把那个人扔出船外去，然后再从1开始数.基督徒想把自己人都留住，他们应该站到什么位置上？②答案是，圈子的次序须安排如下：

CCCCTTTTTCCTCCCTCTTCCTTTCTTCCT，

其中 *C* 代表基督徒，*T* 代表土耳其人.这个次序可借助于下边一句暗语里元音字母的顺序而记住

From numbers' aid and art，never will fame depart，

其中 *a*，*e*，*i*，*o*，*u* 分别代表1,2,3,4,5.于是队伍依次是 *o* 个基督徒，*u* 个土耳其人，等等.

如果每数到十就把那个人扔出船外去，帮助记忆的暗语是③：

Rex paphi cum gente bona dat signa serena.

这个死难问题的一个东方的提法大致如下：从前有一个富农，他有30个孩子，其中15个是已故的前妻所生，其余15个是继室所生.这后一妇人很想让她自己所生的最年长的儿子继承财产.于是，有一天她向他说：“亲爱的丈夫，你就要老了.我们应

---

① 共41个人.这样一来，最后剩下的两个人就是约瑟夫斯和赫格西帕斯.——译者注

② 巴协，问题XXIII，p.174.这个问题先前曾由塔尔塔利亚宣述过.

③ 此语意为“众神之首维纳斯为万民的幸福而安详地注视着”.重要的是元音字母序列.相应的队伍是 *CCTCCCTTTTTCCTTCCCCTCTTTCTTCT*.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



当定下来谁将是你的继承人.让我们把我们的30个孩子排成一个圆圈,从他们中的一个数起,每逢到10就让那个孩子站出去.直到最后剩下哪个孩子,哪个孩子就继承你的财产吧!"这个建议似乎没有什么不公之处.当剔选过程不断进行下去的时候,这个农夫愈来愈感到惊诧,因为他注意到前14个被剔出去的孩子都是前妻所生,而且下一个将要站出去的仍是前妻所生的孩子.
所以他提出从这个孩子开始倒回去数看看情况如何.迫于要马 [33]
上作出决定,并且想到她的孩子们有15比1的有利机会,她立即同意了丈夫的动议.到底谁做了继承人呢?①

一般情况下,把 n 个人排成一个封闭的圆圈,要从中一个一个往外剔.从任意哪个人开始绕着圈不断地往下数,每数到第 m 个人就把他剔出去,直到剩下 r 个人为止.假定这些人中有一个开始时占着第 p 个位置.如果增添一个人,即开始有 $n+1$ 个人,那么,当 $p+m$ 不大于 $n+1$ 时,他应该开始时占据第$(p+m)$个位置,当 $p+m$ 大于 $n+1$ 时,他应该开始时占据第$(p+m-n-1)$个位置.于是,如果剩下的是 r 个人,那么当开始的队伍每增加一个人时,他们皆须由原先的位置沿圆圈向前移过 m 个位置②.

现在假定开始时有 n 个人而最后一个$(r=1)$存活的人在开始时占有第 p 个位置,并且当人数增为 $n+x$ 时,这个人要仍想存活的话应该改占第 y 个位置.那么,若限于考虑使 y 小于 m 的最小的 x 值,则应有 $y=(p+mx)-(n+x)$.

根据这个定理,对于任何特定的 n 值,我们可以很快算出来最后一个存活者开始必须占在第几个位置上.泰特(P.G. Tait)对于开始时占据第 $p(<m)$ 个位置的人,要想使他成为最后的存活者,已经找出 n 应取的值.于是,重复引用上述定理,

---

① 容易试出,结果是前妻所生的那个孩子.——译者注

② P.G. Tait, Collected Scientific Papers, Cambridge, Vol. II, 1900, pp. 432—435.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

他进而对于中间的那些值得出存活者所占的位置.

以约瑟夫斯问题为例,其中 $m=3$. 我们知道 41 个人中最后存活者当初占的是第 31 个位置. 假定开始的人数改为 $(41+x)$,最后存活者开始时在第 y 个位置上. 那么,如果只考虑使 y 小于 m 的最小的 x 值,则 $y=(31+3x)-(41+x)=2x-10$. 现在,我
[34] 们要取使 y 为正数且小于 m 的 x 值. 这样的 x 值只有一个 6,相应的 y 值为 2. 所以,如果总共有 47 个人,那么最后存活的人开始时必须站在第二个位置上. 相仿地,假定开始的人数改为 $47+x$,最后存活者开始时在第 y 个位置上. 在同样的条件下应有 $y=(2+3x)-(47+x)=2x-45$. 于是 $x=23$, $y=1$. 所以,如果总共有 $47+23=70$ 个人,那么最后存活的开始时必须站在第一个位置上. 依此类推,易知若 n 不超过 2 000 000,则当 $n=4,6,9,31,70,105,355,799,1\,798,2\,697,9\,103,20\,482,30\,723,69\,127,155\,536,233\,304,349\,956,524\,934$ 或 787 401 时,最后存活的人开始时都是站在第一个位置上;当 $n=2,3,14,21,47,158,237,533,1\,199,4\,046,6\,069,13\,655,46\,085,103\,691,1\,181\,102$ 或 1 771 653 时,最后存活的人开始时都是站在第二个位置上. 利用这些结论,再重复引用上述定理,可以对于任何中间的 n 值找出最后存活的人开始时所站的位置. 例如, $n=1\,000$ 时, $p=604$; $n=100\,000$ 时, $p=92\,620$; $n=1\,000\,000$ 时, $p=637\,798$. 这些是公司中一位精明的数学家在裁员时会选取的位置.

相仿地,如果有 100 个人遭抽杀,活到最后的人开始时的位置是第 91 号. 因而,如果受戮的是 227 人,活到最后的人开始时的位置应为第 209 号①.

有人提出了原问题的一些修改了的提法. 例如②,让 5 位基督徒和 5 位土耳其人按次序 *TCTCCTCTCT* 排成一个圆圈. 假若

① 原书谓为第 26 号及第 1 号,不妥.——译者注

② H.E. Dudeney, Tit - Bits, London, Oct. 14 and 28, 1905.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

从第 a 个人开始，把每第 h 个人拉出去，所有的土耳其人都被拉去受惩罚，但若从第 b 个人开始，把每第 k 个人拉出去，所有的基督徒都被拉去受惩罚．求 a,b,h,k．一组解是 $a=1,h=11,b=9,k=29$．

我提一个类似的问题．求 c 个土耳其人和 c 个基督徒的一个那样的环形排列，若从某人（譬如说第一个人）开始，每第 h 个人被拉出，则所有的土耳其人将都被拉出去，但若仍从那个人开始，把每第 k 个人拉出，则所有被拉出去的将都是基督徒．这 [35] 是一个很有趣的问题．可以想象那个挑选牺牲者的刽子手有可能弄混了 k 和 h，因而没有把他本来该拉出去的人拉出去，反而把他的朋友们都行了死刑．这个问题实质就是对于给定的 c，求人群的环形排列与相应的适当的 h 值和 k 值．显然，若 $c=2$，则对于排列 *TCCT* 的解是 $h=4,k=3$．若 $c=3$，则对于排列 *TCTCCT* 的一组解是 $h=7,k=8$．若 $c=4$，则对于排列 *TCTTCTCC* 的一组解是 $h=9,k=5$．斯温丹(Swinden)先生曾指出，一般地，若有 $2c$ 个人，其中 c 个开始时接连站在第 $c,c+1,\cdots,2c-1$ 号位置上，h 为 $c+1,c+2,\cdots,2c-1$ 的最小公倍数，则这 c 个人将全被拉出去；若 $k=h+1$，则另外的 c 个人将全被拉出去．诚然，对于它种环形排列，问题是有较简单的解的．如果要求把 n 个指定的人按一定的次序一个个都拉出去，这样的问题可能是无解的．

尼姆游戏与类似的游戏①

一些游戏是由两个人 A 与 B 玩的，有一堆或几堆筹码，按约定，各人轮流取走一些或全部筹码，取得最后一个筹码为赢．前边所述第三个中古时代的算术问题就是一个例子，其中仅有一堆筹码，每次可以取走 1 至 m 个筹码．许多此类游戏皆可用

① 本节的此段文字是由史密斯(C.A.B.Smith)热情提供的．

我们必须知道，而且我们必将知道

http://maths352.bokee.com



斯普拉格(R. Sprague)－格伦迪(P.M.Grundy)数[①] $G(C)$予以分析.对于空位置0,那里没有筹码,$G(0)=0$.对于数目分别为$x,y,\cdots$的筹码堆的任意组合 $C=(x,y,\cdots)$,假定有容许的取
[36] 法使 C 变成别的组合$D,E,\cdots$,则 $G(C)$是异于 $G(D),G(E)$,$\cdots$的最小非负整数.这样就以归纳的方式定义了游戏规则所容许的一切组合 C 的 $G(C)$.依此,在第三个中古时代的问题里,我们找到 $G(x)=$用 $m+1$ 除 x 时的余数.

若 $G(C)>0$,下一个人,譬如说 A,只要取码使局势走向一个"安全的"组合 S 使$G(S)=0$就能确保获胜了.因为按 $G(S)$的定义,或者 S 是空位置,此时 A 已获胜,或者对手 B 必须走到一个新的"不安全的"位置 U,$G(U)>0$,这就回到了讨论开始的情况.游戏以有限的步数结束而 A 获胜.

在尼姆(Nim)游戏[②]里可有任几堆筹码,每个参加者轮流选定一堆并从该堆中随意取多少个(至少一个)筹码.$G(x,y,\cdots)$这时就是$x,y,\cdots$的"尼姆和",其中的尼姆加法运算的定义如下.把$x,y,\cdots$换写为二进制数.然后相加而暂勿进位.最后将每位上的和数换为用2除后的余数,将此结果视为二进制数.例如求尼姆和:$3+_{\text{nim}}7+_{\text{nim}}9$.列式如下:

十进制的3＝二进制的	11
十进制的7＝二进制的	111
十进制的9＝二进制的	1001
相加但不进位	1123
尼姆和	1101＝十进制的13
	＝$G(3,7,9)$

① R. Sprague, Tohoku Journal of Mathematics, 1936, Vol. XLI. p.438; P.M.Grundy, *Eureka*, 1939, Vol. Ⅱ, p.6.

② C.L. Bouton, Annals of Mathematics, 1902, series 2, Vol. Ⅲ, pp.35—39.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

事实上尼姆和满足斯普拉格－格伦迪数的条件.证明实际归结于说明“若 $G(C)>h\geqq 0$,则存在着由 C 到某个组合 D 的走动,这里 $G(D)=h$”.例如,在上列例子中,取 $h=$ 十进制的 11＝二进制的 1011.它与 $G(C)=1101$ 不同的是中间两位数码.把第二堆筹码的个数由 7＝0111 减为 1＝0001 就完成了尼姆和所需的变化,于是 $D=(3,1,9)$,$G(D)=11$.这样的变化总是可能的.安全的组合是那些尼姆和为零的组合,例如,两堆筹码时的 (x,x),三堆筹码时的(1,2,3),(1,4,5),(1,6,7),(2,4, [37]
6),(2,5,7)与(3,4,7).在这些三数组中,任一个数都是其余两个数的尼姆和:$1+_{\mathrm{nim}}2=3$,$1+_{\mathrm{nim}}3=2$,等等.由此推出,例如,$(1+_{\mathrm{nim}}3)+_{\mathrm{nim}}(7+_{\mathrm{nim}}5)=2+_{\mathrm{nim}}2=0$,所以(1,3,7,5)是一个尼姆意义上安全的组合.

在“有约束的尼姆游戏”里,一位参加者从某一堆里取去 m 个筹码.$G(x,y,\cdots)$ 是 $x',y',\cdots$ 的尼姆和,其中 $x',y',\cdots$ 分别是用 $m+1$ 除 $x,y,\cdots$ 所得的余数.更一般地,若尼姆游戏的修改是限制每次取走的筹码数必须是正整数的某个容许的集合中的数,这时 $G(x,y,\cdots)$ 是 $G(x)$,$G(y)$,$\cdots$ 的尼姆和,其中 $G(x)$ 是单独一堆 x 个筹码的斯普拉格－格伦迪数.例如,取的个数必须是一个完全平方数,我们发现,视以 5 除 x 时余数为 0,1,2,3 或 4 而 $G(x)=0,1,0,1,2$.由此可以导出在多于一堆筹码的游戏里的安全组合.

穆尔游戏① 穆尔(E.N.Moore)的尼姆和 Nim_k 的规则和普通的尼姆和 Nim(即 Nim_1)的规则基本上是一样的,唯一不同的是参加者每一步可以从任意几(不超过 k)堆中取筹码.如果把数字 $x,y,\cdots$ 换写成二进位数而作不进位的加法时,和的每个数位上的数码都是 $k+1$ 的倍数,则此组合 $(x,y,\cdots)$ 为安全的.如果把 Nim_k 的规则修改为取走最后一个筹码为输,那么安全组

① Annals of Mathematics, 1910, series 2, Vol. XI, pp.90—94.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

合不变，除了当所有的堆都只有一个筹码时，堆的数目比 $k+1$ 的一个倍数多一.

如果把 Nim_k 再作进一步的修改，限制从每一堆上取走筹码的数目必须是某一“容许集合”中的一个数，那么一般的分析是困难的. 但若仅有 $k+1$ 个堆，其筹码数目分别是 $x_1, x_2, \cdots, x_{k+1}$，且最后一个取筹码者为赢，则一个安全组合符合规律 $G(x_1) = G(x_2) = \cdots = G(x_{k+1})$. 如果堆数少于 $k+1$，则所有的 $G(x_r)$ 都必
[38] 须为零.

凯尔斯游戏① 这个游戏里玩的是一行筹码. 每步取走一个或相邻的两个筹码. 这样可能把一行断成两个较短的行. 取走最后一个筹码为赢. 规律 $G(x, y, \cdots)$ 为 $G(x), G(y), \cdots$ 的尼姆和仍成立. $x = 0, 1, 2, \cdots$ 时 $G(x)$ 的值依次为 0, 1, 2, 3, 1, 4, 3, 2, 1, 4, 2, 6, 4, 1, $\cdots$. 盖伊(R.K.Guy)曾证明，从 $x = 71$ 往后这个序列是有周期的，周期为 12. 在“复式凯尔斯(Kayles)游戏”里，参加者可以每次取相邻的两个或三个筹码. 这时 $G(x)$ 的序列变成 0, 0, 1, 1, 2, 2, 3, 3, 1, 1, $\cdots$，也就是简单凯尔斯游戏的 $G(x)$ 序列中的每一项都重复一次. 如果取筹码的规则是每次取相邻的两个或者孤立的一个，那么 $G(x)$ 的序列将是 0, 1, 1, 0, 2, 1, 3, 0, 1, 1, 3, 2, 2, 3, $\cdots$；从 $x = 33$ 以后它是周期的，周期为 34.

威索夫游戏 威索夫(W.A.Wythoff)②发明一个有两堆筹码的游戏. 参加者可以随意从哪一堆中任取几个或从两堆中各取同样多的筹码. 取得最后一个筹码为赢. 第 r 个安全组合是 $(x, x+r)$，其中 x 是 $\tau r = \frac{1}{2}(\sqrt{5}+1)r$ 的整数部分，因而 $x+r$

---

① S. Loyd, Cyclopedia of Tricks and Puzzles. New York, 1914, p. 232; R.K. Guy 与 C.A.B. Smith, Preceedings of the Cambridge Philosophical Society, 1956, Vol. LII, p.514.

② Nieuw Archief voor Wiskunde, 1907, p.199. 又见 H.S.M. Coxeter, Scripta Mathematica, 1953, Vol.XIX, pp.135—143.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

是 $\tau^2 r$ 的整数部分. 在这些安全组合里,每个正整数出现一次,所以在任两个相邻的正整数或者两个都是 τ 的整倍数或者一个是 τ 的整倍数而另一个是 τ^2 的整倍数. 奥贝恩(T. H. O'Beirne)曾经指出,如果参加者取得最后一个筹码为输,那么安全组合中除了须把(1,2)换为(0,1)与(2,2)之外,其他不变[①].

自从毕达哥拉斯(Pythagoreans)开始研究正五边形并算出其对角线与边长之比以来,$\tau = \frac{1}{2}(\sqrt{5}+1) = 1.6180339887\cdots$ 这个数吸引了许多数学家和业余的数学爱好者. 我们将在第 57 和 137 页上再次遇到它. 它的精微的性质之一属于用有理数逼近 [39]
一个给定的无理数 ξ 的理论. 胡尔维茨(A. Hurwitz)[②]的一个定理说,若 $0 < c \leqslant \sqrt{5}$,则有无穷多个有理数 h/k 适合

$$|\xi - h/k| < 1/ck^2;$$

但若 $c > \sqrt{5}$,则有一些无理数,其中之一便是 τ,相应地仅有有限个有理数适合此不等式.

附　　录

对第 15 页上拼凑问题的注记. 十个数码问题的解是 $35/70 + 148/296 = 1$ 或 $.0123\dot{4} + .9876\dot{5} = 1$,和 $50 + 49 + 1/2 + 38/76 = 100$. 九个数码问题的一个解是 $1.23\dot{4} + 98.76\dot{5} = 100$ 或 $97 + 8/12 + 4/6 + 5/3 = 100$;另一个更漂亮的解[为彼列尔曼[③](Perelman)所给出]是 $1+2+3+4+5+6+7+8\times 9 = 100$,其中

---

① T. H. O'Beirne, Puzzles and Paradoxes, Oxford, 1965, pp. 109, 134—138.

② K. Chandrasekharan, An Introduction to Analytic Number Theory, Berlin, 1968, p. 23.

③ 关于其他几百个解,见 Sphinx, 1935, pp. 95, 111, 112, 124, 125.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

九个数码按自然顺序出现.

对第 27 页上第二个中古时代的算术问题的注记.在所述条件下,等分 24 盎斯为三份的办法有好几种.最漂亮的是哈伯(E.A.Harber)所给的解:

容器可盛	24 两	13 两	11 两	5 两
原盛量	24	0	0	0
第一步	8	0	11	5
第二步	8	5	11	0
第三步	8	13	3	0
[40] 第四步	8	8	3	5

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第2章 算术趣谈

我在这一章里叙述几个算术谬论，个别补充问题，和高等算术里一两个问题.

算术谬论

我从叙述几个证明[①]的例子开始，它们的结论显然都是不可能的.这里包括算术的证明，也包括代数的证明.有几个谬论太明显了，在编写本书的第一版和第二版时，我觉得不值得把它们写进去.但因后来有些来函表示反对，我现在把它们写出来，值得也罢，不值得也罢.

---

① 下文所给的谬论中，第一个和第二个是众所周知的，第三个也不新奇，不过据我的记忆，它最早出现在我的著作《代数》(Cambridge，1890，p.430)里；第四个见于克里斯托尔(G. Chrystal)所著 Algebra(Edinburgh，1889，Vol.Ⅱ.p.159)里；第六个是沃克(G.T.Walker)给出的，我相信除本书之外别的著作里尚未出现过；第七个是达朗贝尔(J.D'Alembert)给出的；第八个是高尔顿(F.Galton)给出的.值得记述的是(i)沙特尔(R.Chartres)在 Knowledge(July，1891)里给出了 $1=2$ 的一个力学的证明和(ii)贝特朗(J.L.F.Bertrand)曾指出 $1=-1$ 可得自积分演算的一个命题：若积分的上、下限皆为常数，则积分的次序可以交换；从而函数 ϕ 的先对 y 积分(从 $y=0$ 到 $y=1$)然后再对 x 积分(从 $x=0$ 到 $x=1$)应等于 ϕ 的先对 x 积分(从 $x=0$ 到 $x=1$)然后再对 y 积分(从 $y=0$ 到 $y=1$)，若取 $\phi=(x^2-y^2)/(x^2+y^2)^2$，则得 $\frac{1}{4}\pi=-\frac{1}{4}\pi$.

我们必须知道，而且我们必将知道

谬论之一 最古老的、也是不大有趣的例子之一是:设 $a=b$,则 $ab=a^2$.

$\therefore\quad ab-b^2=a^2-b^2.\quad\therefore\quad b(a-b)=(a+b)(a-b).$

$\therefore\quad b=a+b.\quad\therefore\quad b=2b.$

$$\therefore\quad 1=2.$$

谬论之二 另一个例子[这是约翰·伯努利(John Bernoulli)

[41] 出的点子]是:因 $(-1)^2=1$,取对数,得

$$2\log(-1)=\log1=0.$$

$$\therefore\quad \log(-1)=0.\quad\therefore\quad -1=e^0.\quad\therefore\quad -1=1.$$

这个议论也可以表述如下:设 x 为适合方程 $e^x=-1$ 的任何值.两端平方,得 $e^{2x}=1$.

$$\therefore\quad 2x=0.\quad\therefore\quad x=0.\quad\therefore\quad e^x=e^0.$$

但 $e^x=-1$ 而 $e^0=1$,故 $-1=1$.

上边两个例子的谬误是明显的,但下边的例子中的谬误隐蔽得要好一些.

谬论之三 大家知道

$$\log(1+x)=x-\frac{1}{2}x^2+\frac{1}{3}x^3-\cdots.$$

当 $x=1$ 时,这级数是收敛的,所以

$$\log2=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\frac{1}{6}+\frac{1}{7}-\frac{1}{8}+\frac{1}{9}-\cdots.$$

$$\therefore\quad 2\log2=2-1+\frac{2}{3}-\frac{1}{2}+\frac{2}{5}-\frac{1}{3}+\frac{2}{7}-\frac{1}{4}+\frac{2}{9}-\cdots.$$

合并分母相同的项,得

$$\begin{aligned}2\log2&=1+\frac{1}{3}-\frac{1}{2}+\frac{1}{5}+\frac{1}{7}-\frac{1}{4}+\frac{1}{9}+\cdots\\&=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\cdots\\&=\log2.\end{aligned}$$

所以 $2=1$.

http://maths352.bokee.com

谬论之四 这个谬论和上一个非常相仿.

$$\begin{aligned}\log 2 &= 1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\frac{1}{6}+\cdots\\ &=\left(1+\frac{1}{3}+\frac{1}{5}+\cdots\right)-\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots\right)\\ &=\left\{\left(1+\frac{1}{3}+\frac{1}{5}+\cdots\right)+\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots\right)\right\}\\ &\quad -2\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots\right)\\ &=\left\{1+\frac{1}{2}+\frac{1}{3}+\cdots\right\}-\left(1+\frac{1}{2}+\frac{1}{3}+\cdots\right)\\ &=0.\end{aligned}$$

谬论之五 由$\sqrt{a}\times\sqrt{b}=\sqrt{ab}$,得 [42]

$$\sqrt{-1}\times\sqrt{-1}=\sqrt{(-1)(-1)}.$$

$$\therefore\quad (\sqrt{-1})^2=\sqrt{1},\quad 即\quad -1=1.$$

谬论之六 下边的证明的根据是一个代数恒等式.本例只能引起熟悉这个恒等式的读者的兴趣.恒等式

$$\sqrt{x-y}=i\sqrt{y-x} \qquad \text{(i)}$$

中 i 代表 $+\sqrt{-1}$或$-\sqrt{-1}$.既然是一个恒等式,不论 x 与 y 代表什么数,它都是对的.先令 $x=a$, $y=b$,得

$$\sqrt{a-b}=i\sqrt{b-a}. \qquad \text{(ii)}$$

再令 $x=b$, $y=a$,得

$$\sqrt{b-a}=i\sqrt{a-b}. \qquad \text{(iii)}$$

又因(i)是一个恒等式,故(ii)与(iii)中的 i 应该是一样的,即,都是 $+\sqrt{-1}$ 或都是 $-\sqrt{-1}$.所以由(ii)与(iii)得到

$$\sqrt{a-b}\,\sqrt{b-a}=i^2\sqrt{b-a}\,\sqrt{a-b},$$

$$\therefore\quad 1=i^2,$$

即

$$1=-1.$$

我们必须知道，而且我们必将知道

http://maths352.bokee.com

谬论之七 下边的谬论是达朗贝尔①给的．大家知道，如果两个数的乘积等于另两个数的乘积，那么这四个数必是成比例的，又从比例式的定义知道，如果第一项大于第二项，那么第三项也必大于第四项．譬如，若 $ad=bc$，则 $a:b=c:d$，且在此比例式中若 $a>b$，则 $c>d$．现在令 $a=d=1$，$b=c=-1$，那么这四个数是适合 $ad=bc$ 的，而且 $a>b$；于是应有 $c>d$，即 $-1>$
[43] 1．这是荒谬的．

谬论之八 概率的数学理论也能引出种种似是而非的论断．我来给出几个这样的例子．

假定②抛起几枚硬币，并注意观察各枚落下后是国徽向上或是麦穗向上．三枚都是国徽向上的概率显然是$(1/2)^3$，即 1/8；相仿地，三枚都是麦穗向上的概率也是 1/8；所以，三枚落下相同（都是国徽向上或者都麦穗向上）的概率是 1/4．可是，抛起的三枚硬币落下后，至少有两枚是一样的；而第三枚落下后国徽向上的概率是 1/2，麦穗向上的概率也是 1/2．所以第三枚和另两枚落下后相同的概率是 1/2．由此可知三枚落下后全一样的概率应该是 1/2．请读者说这两个矛盾的结论是否都对？ 如否，哪个对？

第二张幺的悖论 假定玩桥牌或惠斯特③时一个人声称在发给他的 13 张牌中有一张幺（即 A）．设他手中还有另一张幺的概率是 p．然而，如果他声称在发给他的 13 张牌中有一张是红心幺，那他手中还有另一张幺的概率 q 是大于 p 的．因为④包括一张幺的套数是 $\binom{52}{13}-\binom{48}{13}$，而包括两张幺的套数是 $\binom{52}{13}-$

---

① Opuscules Mathematiques, Paris, 1761, Vol. I, p. 201.

② 见 Nature, Feb. 15, March 1, 1894, Vol. XLIX, pp. 365—366, 413.

③ 惠斯特（whist）为桥牌的前身．——译者注

④ 这个议论是德勒里（D.B.De Lury）给出的．

我们必须知道，而且我们必将知道

$\binom{48}{13}-\binom{48}{12}$，所以 $p=1-4\binom{48}{12}\Big/\left\{\binom{53}{13}-\binom{48}{13}\right\}=\frac{5359}{14498}$. 但是包括红心幺的套数是 $\binom{51}{12}$，而包括红心幺和另一张幺的套数是 $\binom{51}{12}-\binom{48}{12}$；所以 $q=1-\binom{48}{12}\Big/\binom{51}{12}=\frac{11686}{20825}$. 于是 $p<\frac{1}{2}<q$，乍一看这似乎是荒谬的.

圣彼得堡悖论[1] 下边是一个著名的例子. 将一枚硬币抛 [44]
落，如果国徽向上，就结束，如果麦穗向上，就再抛. 若第一次就出现国徽，庄家就付给赌徒 1 元；若第二次才出现国徽，庄家就付给赌徒 2 元；若第三次才出现国徽，庄家就付给赌徒 4 元；如此下去，每次付加倍的钱. 如果直到第 n 次才出国徽，赌徒将得到 2^{n-1} 元. 赌徒应先向庄家交多少钱时取得赌博的资格才公平？

赌徒有 1/2 的机会得到 1 元，有 1/4 的机会得到 2 元，等等. 所以他可以有理由抱得到总钱数为

$$\frac{1}{2}\cdot 1+\frac{1}{4}\cdot 2+\cdots+\left(\frac{1}{2}\right)^n 2^{n-1}+\cdots=\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\cdots,$$

即，无限多元的期望.

为了使答案是有限的数字，在对此赌博规则的各种修改方案中，最令人满意的方案之一是 G·克莱姆(Gabiel Cramer)(大约在 1730 年)致尼古拉斯·伯努利(Nicolas Bernoulli)[2]的一封信中所提出的. 克莱姆假定庄家的本钱是有限的，譬如说，为 2^{24} 元. 只要 $n<25$，赌徒就有 $1/2^n$ 的机会在第 n 次抛币时赢得 2^{24} 元. 因为

$$\sum_{1}^{24}\frac{2^{n-1}}{2^n}+\sum_{25}^{\infty}\frac{2^{24}}{2^n}=12+1=13,$$

---

① 参看 E. Kamke, Einführung in die Wahrscheinlichkeitslehre, Leipzig, 1932, pp. 82—89.

② Isaac Todhunter, A History of the Mathematical Theory of Probability, London, 1865, p. 221(art. 391).

http://maths352.bokee.com

[redacted]

所以赌徒的期望是 13 元，也就是应该先交纳给庄家的资格费，这是一个合理的款数.

其他概率问题

这里要说的是一个使许多人惊诧的结果(哈罗尔德·达文波特(Harold Davenport)给出的). 如果你调查一下多于 23 个人的生日，你会发现多半有两个人是相同的(包括月份和日子). 试考虑 n 个人的生日全不相同的概率，即，由 365 天里任意选出 n
[45] 天(每次都由 365 天里选一天)而每次都不相同的概率. 总的可能的选择的组合共有 365^n 种，而没有两天相同的组合共有 $365\cdot364\cdot\cdots\cdot(365-n+1)$ 种，故所求的概率①为 $365\cdot364\cdot\cdots\cdot(365-n+1)/365^n$. 当这个表达式等于 1/2 时，即当

$$\left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\cdots\left(1-\frac{n-1}{365}\right)=\frac{1}{2}$$

时，上述事件发生与否的可能性是一样的. 取对数后，得到近似的关系

$$\frac{1}{365}+\frac{2}{365}+\cdots+\frac{n-1}{365}=\log_e 2,$$

或 $n(n-1)=506$，由此得到 $n=23$.

重排 下边的问题②有点类似. 假定你给 n 位朋友各写了一张信和相应的 n 个信封. 也许你竟会弄出非常遗憾的错误——每张信纸都装错了信封，这样错误的情况可能有多少?

---

① 作为检验，注意当 $n=366$ 时此式等于零.(为简单计，我略去了出生于 2 月 29 日的可能性；除去这个特殊情况，并不影响结论.)

② 参看 P.R. de Montmort, Essai d'analyse sur les jeux de hasard, Paris, 1713, p.132; J.L.Coolidge, An Introduction to Mathematical Probability, Oxford, 1925, p.24; C.V. Durell and Alan Robison, Advanced Algebra, London, 1937, p.459. 又见 A.C. Aitken, Determinants and Matrices, Edingburgh, 1956, p.135.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

设有 X_n 种情况.假定第一张信装进第 a 个信封里了而第 b 张信装进第一个信封里了.若 $a=b$,那么还有 $n-2$ 张信有待错误地装进 $n-2$ 个信封里去,用 X_{n-2}表示这种错误情况的数目.由于 $a(=b)$可以取从 2 到 n 的任何一个值,所以此类情况共有$(n-1)X_{n-2}$种可能.在任何它种情况里,$a \neq b$.暂且固定 b 而令 a 跑过从 2 到 n 除 b 之外的值.在这除第一个之外的 $n-1$ 个信封里,还需把除第 b 张之外的信全都错误地装进去,而且不要把第一张装进第 b 个信封里.这样的情况恰有 X_{n-1}种,因为只要把第 b 个信封看成是第一张信的正确信封,这就正是在原先的问题中把 n 换成 $n-1$ 所成的问题.再让 b 跑遍从 1 到 n [46]
除 a 之外的值,共得$(n-1)X_{n-1}$种情况.所以

$$X_n=(n-1)(X_{n-1}+X_{n-2}).$$

这个关系①立即给出相继的数字.显然 $X_1=0$ 且 $X_2=1$;于是 $X_3=2, X_4=9, X_5=44, X_6=265$,等等.明显公式是

$$X_n = n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\cdots\pm\frac{1}{n!}\right)$$

(“次阶乘”).

因为 n 张信往 n 个信封里装的配合总共有 $n!$种,所以上述非常遗憾之事发生的概率是

$$\frac{X_n}{n!}=1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\cdots\pm\frac{1}{n!}.$$

等号右边的式子是 $e^{-1}(=0.367879\cdots)$的级数表达式,所以我们可以说这个概率近似地等于 $1/e$.误差限是 $1/(n+1)!$,当 $n=6$ 时大约为 0.0002.

如果拿两副扑克牌(其中一副是洗好的)一张一张顺次对比一下,问一对也没碰上相同的牌的概率是多少?这不过是上述问题的另一个具体的说法;答案是 $1/e$(误差小于 10^{-69},

① 一个更简单的关系是 $X_n=nX_{n-1}+(-1)^n(X_1=0)$.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

因为一副扑克牌是 52 张). 许多人要打赌认为决不会碰上相同的牌,但是只要知道 $e>2$,一个不那么精明的人反而可能会赢.

杂题 我可以再补充几个典型问题,或谓之游戏.

第一个问题如下:两位职员 A 与 B 受雇,A 的工资是第一年 100 镑,半年发一次工资,每年递增 20 镑,B 的工资也是第一年 100 镑,半年发一次工资,每半年递增 5 镑. 问谁的收入多? 答:B 的收入多. 因为在第一年里 A 收入 100 镑,B 收入第一次 50 镑,第二次 55 镑,共计 105 镑. 第二年 A 收入 120 镑,B 第一
[47] 次收入 60 镑,第二次收入 65 镑,共计 125 镑. 显然 B 每年多收入 5 镑.

另一个简单的算术问题是:一教堂的圣歌牌上有四条横槽,槽里公布着要演唱的圣歌的号码. 所用的圣歌书上共载 700 首圣歌. 假定每块号码板上只有一个数码. 问库房里至少应备有多少块号码板,才能把任意挑选的四首不同的圣歌的号码都公布出来? 如果可以把 6 倒过来当 9 用,对于结果有何影响? 答案是 86 和 81. 如果每块板的正反两面都漆上数码,答案又是什么?

作为又一个问题,请往下看. 一个人把他的钱财的 $1/n$ 押作一项输赢机会均等(譬如抛硬币落下后哪一面向上)的赌注. 他一次又一次地这样玩下去,每次都把他当时所有的钱的 $1/n$ 押上去. 如果玩到不玩了,他输的次数和赢的次数相等,那么他这场赌博是有所得呢还是有所失? 实际上他有所失.

这里是另一个简单的问题,我经常收到它的错误答案. 一个大玻璃杯里盛着半杯酒,另一个大玻璃杯里盛着半杯水. 从第一个杯子里舀一茶匙酒倒进盛着水的那个大杯里. 搅匀后,再从第二个大杯里舀一茶匙水酒混合液送回第一个大杯里去. 经过这么一来一往两下子之后,问原来盛水的杯子里的酒比盛酒的杯子里的水多呢、少呢、还是一样多? 每次问时,总是有多数人回

我们必须知道，而且我们必将知道

http://maths352.bokee.com

答盛水的杯子里的酒比盛酒杯子里的水多.可是事实不是那样.

排 列 问 题

排列与组合方面的许多问题都是颇有趣的.用很少几件东西作成的组合的方式的数目可能非常大.我可以举两个很简单的例子.12根长度相等而颜色不同的杆做成一个立方体的骨架,其方式有199 548 00种①;一副52张的扑克牌分给四位牌手的可能的不同方式数是$(52!)/(13!)^4$,即,53 664 737 765 488 792 [48]
839 237 440 000.

投票问题 这里是两个简单的例子.(i)设有两位候选人,甲得a票,乙得b票($a>b$).在唱票过程中,甲得的票数一直保持领先于乙得的票数的概率是$(a-b)/(a+b)$.(ii)假定有p个选举人,每人可投r票,但这r票中至多只能把s票投给同一位候选人,要选出的人数为n.那么一位候选人要获胜的话,他的支持者必须多于$pr/(ns+r)$个.

圆桌骑士② 一个困难得多的排列问题是求由n个人作环形排列的总数,但要其中任一个人在任两种排列中的左、右邻人不得都相同.大家知道,如果没有任何附带条件,那么n个人作成的环形排列可以有$(n-1)!/2$种不同的方式.如果有附带条件——所有的人在各种场合里的左、右邻人不得都相同,那么这样的排列的总数不会超过$(n-1)(n-2)/2$个,因为这是任一指定的人可以坐在从其余的人中每种可能选出的两个人之间的情况的数目.但事实上总可以确定出$(n-1)(n-2)/2$种排列,其中任何两种排列中没有人的两个邻人都相同.

当n取各种不同的值时的解都已经被找到了.下边是当n

---

① Mathematical Tripos, Cambridge, Part Ⅰ, 1894.

② 稗史称古不列颠王Arthur幕下之骑士,环圆桌而坐.游戏之名即本于此.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

= 8时，8 个人的合乎要求的 21 种排列.[①]

1,2,3,4,5,6,7,8；1,2,5,6,8,7,4,3；1,2,7,8,4,3,5,6；
1,3,5,2,7,4,8,6；1,3,7,4,6,8,2,5；1,3,8,6,2,5,7,4；
1,4,2,6,3,8,5,7；1,4,3,8,7,5,6,2；1,4,5,7,6,2,3,8；
1,5,6,4,3,7,8,2；1,5,7,3,8,2,6,4；1,5,8,2,4,6,3,7；
1,6,2,7,5,3,8,4；1,6,3,5,8,4,2,7；1,6,4,8,2,7,3,5；
1,7,4,2,5,6,8,3；1,7,6,3,2,4,5,8；1,7,8,5,6,3,4,2；
[49] 1,8,2,3,7,6,4,5；1,8,4,5,3,2,7,6；1,8,6,7,4,5,2,3；

确定这些排列的方法是冗长的，且远非易事.

入席问题[②] 另一个困难的排列问题是求 n 对配偶围圆桌男女相间而坐的可能安排数，条件是先让 n 个妻子坐到指定的位置上，然后让 n 个丈夫入坐但不许与自己的妻子为邻.

解法涉及不和谐排列[③]的理论且远非易事. 我只想指出 n 不超过10的那些结果. 当 $n = 3$时，$x = 1$；当 $n = 4$时，$x = 2$；当 $n = 5$时，$x = 13$；当 $n = 6$时，$x = 80$；当 $n = 7$时，$x = 579$；当 $n = 8$时，$x = 4\ 738$；当 $n = 9$时，$x = 43\ 387$；当 $n = 10$时，$x = 439\ 792$.

巴协的砝码问题[④]

前一章里所述许多比较容易的问题有些是巴协给出的，其

---

① 此解答是 1906 年五月贝霍尔特(E.G.B.Bergholt)先生告知我的；见 The Secretary and The Queen, August, 1906. 杜德尼(H.E.Dudeney)先生在 1905 年曾经解决了这问题当 $n = 6$ 的情况，并且通知我，比利(E.D.Bewley)先生已经解决了 n 为偶数的情况、而他自己有解决 n 为奇数时的通用方法. 在数学期刊上出现过关于这个问题的各样的文章.

② E.Lucas, Théorie des Nombres, Paris, 1891, pp.215, 491—495.

③ 见 P. A. MacMahon, *Combinatory Analysis*, Vol. I, Cambridge, 1915, pp.253—256；P.Halmos 与 H.E.Vaughan, American Journal of Mathematics, 1950, Vol. LXXII, pp.214—215；D.J.Newman, American Mathematical Monthly, 1958, Vol. LXV, P.611.

④ Bachet，附录，问题Ⅴ，p.215.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

他是他收集在他的古典的 Problèmes 一书里的．他所提出的较难的问题之一是砝码问题：要想在天平上称出从 1 磅到 40 磅在内的任何整磅数，问最少需要几个多重的砝码？巴协给出了两种解答：(i)假定只许把砝码放到天平一端的秤盘里，至少需要六个砝码，重量分别为 1，2，4，8，16，32 磅．塔尔塔利亚[①]在 1556 年已经指出了这个答案；(ii)假定天平两端的秤盘里都可以放砝码，那么，最少可以减到四个砝码，重量分别为 1，3，9，27 磅．

巴协考虑的第二种情况的理由是：要称出 1 磅非有一个 1 [50]
磅的砝码不可．要称出 2 磅，我们需要有一个 2 磅或者一个 3 磅的砝码；可是有了 1 磅和 2 磅的砝码可以称出 1 磅，2 磅和 3 磅，而有 1 磅和 3 磅的砝码可以称出 1 磅，$(3-1)$磅，3 磅和$(3+1)$磅．再有一个 9 磅的砝码，我们就能称出从 1 磅到 13 磅的一切整磅数；可见添一个 9 磅砝码后量程要比添一个任何别的小于 9 磅砝码的量程都大．同理，用 1，3，9，27 磅四个砝码足以称出从 1 磅到 40 磅的一切整磅数．同理，用 $1,3,3^2,\cdots,3^{n-1}$磅的 n 个砝码足以称出从 1 磅到$(1+3+3^2+\cdots+3^{n-1})$即$\frac{1}{2}(3^n-1)$磅的一切整磅数．

当量程给定时，要想确定最少必需配备的砝码，只须把最大的磅数化为进位数，不过在求各位数码时，余数只许是 0，1 或 -1，为此可把余数 2 写成 $3-1$，即将商数增 1，那时余数就是 -1 了．这在多数代数教科书里都有所解释．

巴协的讨论既没有证明他的结论是唯一的，也没有证明他要的砝码个数是最少的．这些纰漏已经由大麦克马洪(Major MacMahon)补正了，他讨论了困难得多的问题(巴协问题是它的一个特例)．他的问题的提法是：允许用相同的砝码，要在下述两

① Trattato de' numeri e misure, Venice, 1556, Vol. Ⅱ, bk. Ⅰ, chap. XVI, art. 32.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

种情况下确定所有可能的足以称出从 1 磅到 n 磅的所有整数磅，(i)砝码必须放在同一个秤盘里；(ii)砝码可以往两个秤盘里放．他还研究了在附加下列两个条件之一或二者时，结论应如何修正．两个附加条件是：(a)没有别的称法；(b)每种重量只有一种称法，即，称法是唯一的①．

[51] 情况(i)的解决的关键是把 $1+x+x^2+\cdots+x^n$ 分解成形状为 $1+x^a+x^{2a}+\cdots+x^{ma}$ 的因子，解的个数取决于 $n+1$ 的合成特征．情况(ii)的解决的关键是把 $x^{-n}+x^{-n+1}+\cdots+x^{-1}+1+x+\cdots+x^{n-1}+x^n$ 分解成形状为 $x^{-ma}+\cdots+x^{-a}+1+x^a+\cdots+x^{ma}$ 的因子，解的个数取决于 $2n+1$ 的合成特征．

巴协的问题属于情况(ii)，$n=40$．麦克马洪的分析表明，要把 $x^{-40}+x^{-39}+\cdots+1+\cdots+x^{39}+x^{40}$ 分解成具有所需形状的因子，可以有八种不同的方式．第一种就是此式的本身，相当于 $a=1, m=40$．第二种，此式等于 $(1-x^{81})/x^{40}(1-x)$，它可以分解成 $(1-x^3)/x(1-x)$ 与 $(1-x^{81})/x^{39}(1-x^3)$ 的乘积；因此它可以分解成两个具有上述形状的因子，一个里 $a=1, m=1$，另一个里 $a=3, m=13$．第三种，相仿地，此式还可以分解成两个那样的因子，一个里 $a=1, m=4$，另一个里 $a=9, m=4$．第四种，它还可以分解成三个那样的因子，一个里 $a=1, m=1$，另一个里 $a=3, m=1$，其余一个里 $a=9, m=4$．第五种，它又可以分解成两个那样的因子，一个里 $a=1, m=13$，另一个里 $a=27, m=1$．第六种，它又可以分解成三个那样的因子，一个里 $a=1, m=1$，另一个里 $a=3, m=4$，其余一个里 $a=27, m=1$．第七种，它又可以分解成三个那样的因子，一个里 $a=1, m=4$，另一个里 $a=9, m=1$，其余一个里 $a=27, m=1$．第八种，它还可

① 见他的文章，发表于 Quaterly Journal of Mathematics, 1886, Vol. XXI, pp. 367—373. 关于这个方法有一篇报告在 Nature, Dec. 4, 1890, Vol. XLII, pp. 113—114.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

以分解成四个那样的因子,一个里 $a=1,m=1$,第二个里 $a=3,m=1$,第三个里 $a=9,m=1$,第四个里 $a=27,m=1$.

这些结果表明,在条件(ii),(a)与(b)之下,有八种可能的砝码组,它们每一组都能够称出从 1 磅到 40 磅的一切整数磅. 如果用 w^p 表示 p 个等于 w 的砝码,那么这八组解就是 1^{40}; $1,3^{13}$; $1^4,9^4$; $1,3,9^4$; $1^{13},27$; $1,3^4,27$; $1^4,9,27$; $1,3,9,27$. 这最后一组正是巴协的解. 它不仅是砝码个数最少的解,而且也是唯一的一组没有相同砝码的解. [52]

1/*n* 的十进制小数表示

米勒(J. C. P. Miller)当他还是一个中学生的时候(大约在 1920 年)曾发明过一个把分数 $1/n$ 表示为循环十进小数的值得注意的技巧. 为了避开讨厌的复杂性,我们假定 n 不能被 2 或 5 整除. 前几位小数须按通常的方式用除法算出. 然后加 1,再除以 2,从而得出 m/n 的小数表达式的前几位,这里 $m=\frac{1}{2}(n+1)$. 若 m 为偶数,则再除以 2;若 m 为奇数,则先加 1,再除以 2. 如此继续下去,直到发现 $1/n$ 的某个倍数的一系列小数位上的数码出现在比该系列在 $1/n$ 的小数位里较前的位置上. $n=19$ 是一个几乎令人焦急的例子:

$$\frac{20}{19}=1.\dot{0}5263157894736842\dot{1},$$

$$\frac{10}{19}=0.\dot{5}2631578947368421\dot{0}.$$

在这个例子里,我们只须把相继的每位小数从第二行移到第一行,然后接下去除以 2.

当 $n=17$ 或 47 时,需用 2 连除三次之后才认出--连串三个数码(印为黑体)提前出现:

$$\frac{18}{17}=1.05\mathbf{882}\cdots,\quad \frac{48}{47}=1.02\mathbf{127}\cdots,$$

我们必须知道，而且我们必将知道

http://maths352.bokee.com



$$\frac{26}{17}=1.52941\cdots,\quad \frac{24}{47}=0.51063\cdots,$$

$$\frac{30}{17}=1.76470\cdots,\quad \frac{12}{47}=0.25531\cdots,$$

$$\frac{15}{17}=0.88235\cdots,\quad \frac{6}{47}=0.12765\cdots.$$

[53] 在这类情况里，不必用 2 连除三次，可用 8 除第一行，然后把数码（一个个或两两）从第四行移到第一行，从而免掉写算第二行和第三行.

当 $n=81$ 时，将 $82/81=1.01234\cdots$ 用 2 连除六次（遇到分子为奇数时先加 1）后，认出数码 234. 后三次的连除可代以用 8 除一次. 下边仅给出第一、第四、第七行：

$$\frac{82}{81}=1.0123456790\cdots,$$

$$\frac{152}{81}=1.8765432098\cdots,$$

$$\frac{19}{81}=0.2345679012\cdots.$$

于是我们断言 $1/81=0.\dot{0}1234567\dot{9}$.

如果我们认出一连几个数码出现在较后的位置上，那么可以把程序修改为：把数码从第一行移到后一行，然后把后者乘以 2（或除以 5），再接到前一行上去. 例如，当 $n=49$ 时我们发现

$$\frac{50}{49}=1.\dot{0}2040816326530612244897959183673469387755\dot{1},$$

$$\frac{25}{49}=0.\dot{5}1020408163265306122448979591836734693877\dot{5}.$$

小数与连分式

每个正数仅可以一种方式表示为一个十进位小数. 如果这数是有理的（即，可以表示为一个普通的分数），则其十进位小数表示是有尽的或者（在若干数位之后）是循环的；否则，例如$\sqrt{2}=$

我们必须知道，而且我们必将知道

http://maths352.bokee.com



1.41421356…或 $\pi = 3.14159265\cdots$，它将是无尽的而且是非循环的.假若采用另一种进位制，那么数码序列当然就完全不同了.一个有理数的“小数”可以在一种进位制里是有尽的而在另一种进位制里是循环的.例如，在七进位制里，$\frac{1}{7} = 0.1$，而不是熟知的 $0.\dot{1}4285\dot{7}$.给定一个按常用进位制表示的整数（十进位数），我们可以把它化为 p 进位数，为此只须用 p 一再去除它，[54]
并注意相继的余数.这些余数倒读时就是所求 p 进位数数码.对于小数来说，规则就不同了.这时要用 p 一再去乘其小数部分，相继出现的整数部分就是所求 p 进位的小数数码（顺序从左到右）.以化至二进位为例，

$$\sqrt{2}(=\sqrt{10}) = 1.0110101000001001111100\cdots,$$
$$\pi = 11.001001000011111101101\cdots.$$

实际计算如下：

1.41421356	3.14159265
0.82842712	0.28318530
1.65685424	0.56637060
1.3137085	1.1327412
0.6274170	0.2654824
1.2548340	0.5309648
0.509668	1.2619296
等等	等等

一连五个零使得 1.0110101 成为 $\sqrt{2}$ 的一个特别好的近似值.事实上，进行二进制的运算，不难发现 $(1.0110101)^2 = 1.11111111111001$.作为 π 的一个良好的近似值，我们注意 $1\dot{1}.00\dot{1} = 3\frac{1}{7}$.

有点相仿的是，每个正数恰可以一种方式表示为**正则连分式**

我们必须知道，而且我们必将知道

http://maths352.bokee.com



$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cdots}}}=a_0+1/a_1+1/a_2+1/a_3+1/\cdots$$

（约定每条斜线/管到后边的整个式子），a 都是正整数，只有 a_0
[55] 可以为零．例如①

$$\sqrt{2}=1+1/2+1/2+1/2+1/\cdots,$$

$$e=2+1/1+1/2+1/1+1/1+1/4+1/1+1/1+1/6+1/1+1/1+1/8+1/\cdots,$$

$$\pi=3+1/7+1/5+1/1+1/292+1/1+1/1+1/1+1/2+1/1+1/3+1/1+1/\cdots.$$

这种表达式在三方面优于小数：(i)有理数的连分式都是有尽的，且二次无理数的连分式都是循环的；(ii)它与任何特定的进位制无关（除了那些偏商 a 本身，自不待言）；(iii)它引出"最佳可能"的有理逼近，其意义将在下章中予以几何说明．

在相继的各个加法步骤上截断连分式所得的有理近似式

$$\frac{b_1}{c_1}=\frac{a_0}{1},\frac{b_2}{c_2}=\frac{1+a_0a_1}{a_1},\frac{b_3}{c_3}=\frac{a_0+a_0a_1a_2+a_2}{1+a_1a_2},\cdots,$$

称为渐近分数．这些渐近分数有许多值得注意的性质．它们适合下列递推公式

$$b_{n+1}=b_{n-1}+a_nb_n,\quad c_{n+1}=c_{n-1}+a_nc_n.$$

例如，$\sqrt{2}$，e 和 π 的前六个渐近分数分别是 $\frac{1}{1},\frac{3}{2},\frac{7}{5},\frac{17}{12},\frac{41}{29},\frac{99}{70}$；$\frac{2}{1},\frac{3}{1},\frac{8}{3},\frac{11}{4},\frac{19}{7},\frac{87}{32}$；$\frac{3}{1},\frac{22}{7},\frac{333}{106},\frac{355}{113},\frac{103\,993}{33\,102}$．

---

① 虽然 $\sqrt{2}$ 和 e 的"偏商"$(a_1,a_2,\cdots)$遵从简单的规律，但是对于 π 还没有发现什么规律．第四商 292 为所知之最大者，其次是 $a_{73}=161$．据雷默（D.H.Lehmer）前一百个商的算术平均数为 10.2；其中有 41 个是一．见帕茨（W.Patz），Tafel der Regelmässigen Kettenbrüche，Berlin，1955．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

一切无理连分式中最简单的是

$$\tau = 1 + 1/1 + 1/1 + 1/1 + 1/\cdots,$$

它适合方程 $\tau = 1 + 1/\tau$，从而(显然 τ 为正数)可知 $\tau = \frac{1}{2}(\sqrt{5} + 1)$.(参看本书第 38 页，威索夫游戏.)它的渐近分数是$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \cdots$，它们的分子与分母都构成斐波那契(Fibonacci)数列.

1,1,2,3,5,8,13,21,34,55,89,144,233,377,….

这数列中的每一个数都等于它前边相邻的两个数的和.据说① [56]
相间的斐波那契数之比等于某种植物枝干上相继生长出的两片叶子旋转的圈数:榆树和菩提树是 1/2，山毛榉和榛树是 1/3，橡树和苹果树是 2/5，白杨和玫瑰是 3/8，柳树和杏树是 5/13，等等.这些分数是

$$\tau^{-2} = 1/2 + 1/1 + 1/1 + 1/1 + 1/\cdots$$

的渐近分数.τ 这个数与正五边形、正十边形、正十二面体、以及正二十面体的度量性质有密切的联系，因为它等于 $2\cos\frac{1}{5}\pi$.如果一个线段被截成的两份，其中一份是另一份的 τ 倍，或者是原线段长的 $1/\tau$，则称这样的分截为黄金分割.通常采用符号 τ 表示它，因为它是希腊字 $\tau o\mu\eta$(“截割”)的第一个字母.第 n 个斐波那契数是

$$\{\tau^n - (-\tau)^{-n}\}/\sqrt{5}.$$

有理直角三角形

若一直角三角形的两腰之比为有理数，我们可以把它取为

① 例如，可参看 H. S. M. Coxeter, Introduction to Geometry, New York, 1969, pp. 169—172.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



两个无公因子的整数之比.据毕达哥拉斯定理,这样一个“本原”三角形的三个边长 x,y,z 适合方程 $x^2+y^2=z^2$,z 为斜边长.此方程的通解(除了显然可以交换 x 与 y 之外)为①

$$x=b^2-c^2,\quad y=2bc,\quad z=b^2+c^2,$$

其中 b 与 c 任意两个互素整数,一奇一偶且 $b>c$.值组 $b=2,c=1$ 给出熟知的 3,4,5 三角形②.数 x 与 z 总是奇数,y 可被 4 整除.x 或 y 可被 3 整除,x,y,z 之一可被 5 整除.因而 xy 可被
[57] 12 整除且 xyz 可被 60 整除.

b	c	x	y	z	$x+y+z$ $=2b(b+c)$	b	c	x	y	z	$x+y+z$ $=2b(b+c)$
2	1	3	4	5	12	5	4	9	40	41	90
3	2	5	12	13	30	7	2	45	28	53	126
4	1	15	8	17	40	6	5	11	60	61	132
4	3	7	24	25	56	8	1	63	16	65	144
5	2	21	20	29	70	7	4	33	56	65	154
6	1	35	12	37	84	8	3	55	48	73	176

上表列举了前十二个本原三角形.它们都在 $z<80$ 且 $x+y+z<180$ 的范围内.D·N·雷默曾证明③斜边小于 X 的本原三角形的个数大约是 $X/2\pi$,且周长小于 X 的本原三角形的个数大约是 $(X\log 2)/\pi^2$.注意 $80/2\pi=12.73\cdots$,而 $(180\log 2)/\pi^2=12.64\cdots$.

若 $b-c=1$,则 $z-y=1$ 上列第一、第二、第四、第七、与第九个三角形就是这样.若 c 与 b 为序列 1,2,5,12,29,70,…中

① G.Chrystal, Algebra, Edingburgh, 1889, Vol.Ⅱ, p.531.

② E.T.Bell, Numerology, Baltimore, 1933, p.26 ff.

③ American Journal of Mathematics, 1900, Vol.XXII, p.38.

http://maths352.bokee.com



相继的两项，即①若 b/c 收敛于连分式

$$\sqrt{2}+1=2+1/2+1/2+1/2+1/\cdots,$$

则 $|x-y|=1$. 上列第一个、第五个三角形就是这样.

奥普诺(F. Hoppenot)曾指出，最大者为 $2n(n+1)$ 的 $n+1$ 个相邻正整数的平方和等于其后边 n 个相邻的 n 个正整数的平方和. 例如 $10^2+11^2+12^2=13^2+14^2$, $21^2+22^2+23^2+24^2=25^2+26^2+27^2$, 等等. 与等式 $3^2+4^2=5^2$ 相仿的另一个类比是 $3^3+4^3+5^3=6^3$. 方程 $x^3+y^3=z^3$ 没有正整数解，方程 $x^4+y^4=z^4$ 也没有正整数解. 欧拉②曾猜想关于方程 $x^4+y^4+z^4=v^4$ 的一个相应的论断：若它有解，则 v 必须大于 1040. 另一方面，x^4+ [58]
$y^4=z^4+v^4$ 却有无穷多解③.

三角形数与金字塔数

三角形数即

$$1,3,6,10,15,21,28,36,45,55,66,\cdots,\frac{1}{2}n(n+1),\cdots,$$

它们之中每一个都是从 1 开始的前几个相邻的正整数的和. 顾名思义，它们是恰好能摆成正三角形的小点(或相等的圆圈)的个数：最上边一个，一个下边摆两个，两个下边摆三个，如此等等. 数

$$1,36,1225,41616,1413721,48024900,\cdots$$

既是三角形数，同时又是平方数. 此类数的一般公式是 b^2c^2, 这里 b/c 是 $\sqrt{2}$ 的连分式的任一渐近分数.

---

① M. Kraïtchik, La Mathématique des Jeux, Brussels, 1930, p. 106.

② Commentationes Arithmeticae Collectae, Petrograd, 1849, Vol. Ⅰ, pp. 473—476; Vol. Ⅱ. pp. 450—456. 是否存在着三个正整数 x, y, z 能使 $x^2+y^2, y^2+z^2, z^2+x^2, x^2+y^2+z^2$ 这四个数都是平方数？尚且不知道.

③ 见 Sphinx, 1937, p. 98.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



相继的三角形数之和为四面体数：

$$1,4,10,20,35,56,84,120,\cdots,\frac{1}{6}n(n+1)(n+2),\cdots,$$

它们是恰能垒成正四面体堆垛的大小相同的小球的个数. 相仿地，相邻的正整数的平方的和为金字塔数：

$$1,5,14,30,55,91,140,204,\cdots,\frac{1}{6}n(n+1)(2n+1),\cdots.$$

相邻的正整数的立方和(从 1 开始)是相应的三角形数的平方. 任两相邻的三角形数之和皆为平方数. 任两相邻的四面体数之和皆为金字塔数.

既是平方数同时又是金字塔数的唯一的数(>1)只有 4 900. 这个结果是由吕卡斯(E. Lucas)在 1875 年猜想而由沃村
[59] (G. N. Watson)在 1918 年证明的①，其证明远非初等的.

可　除　性

如果两个整数 x 与 y 之差为某一正整数 p 的整倍数，则称 x 与 y 为关于模 p 同余，记为

$$x-y\equiv 0(\bmod p)\text{或 } x\equiv y(\bmod p).$$

每个整数恰与 p 个余数 $0,1,2,\cdots,p-1$ 之一同余($\bmod p$). 余数有其算术，它与普通数的算术非常相仿，包括加法、减法、乘法. 例如，以 6 为模时

$$3+4\equiv 1,\quad 3-4\equiv 5,\quad 3\times 4\equiv 0.$$

当模 p 为素数时(本章中以下皆假定如此)，这种算术更为有趣. 素数的定义如下.

素数是那种大于 1 的正整数，它只能被 1 和它自身整除.

---

① E. Lucas, Nouvelles Annales de Math. (2), 1918, Vol. XIV, p. 336; G. N. Watson, Messenger of Mathematics. (new series), 1918, Vol. XLVIII, pp. 1—22.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

(把 1 从素数表里排斥出去，我们就可以断言每个自然数只能以一种形式分解成素因子的乘积．例如 $504 = 2^3 \cdot 3^2 \cdot 7$．)小于 100 的二十五个素数是 2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97．欧几里得曾证明有无穷多个素数存在，他的论证大致如下：考虑直到某个特定的素数 p 的所有素数的乘积 $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p$．显然，$P+1$ 不能被这些素数中的任一个整除．所以它有一个大于 p 的素除数(它自身就可能是)．因此，任意给定一个素数时，都有比它还要大的素数．

企图给素数一个明显公式的最佳尝试是欧拉①提出的二次型 $x^2 + x + 41$，它当 $x = 0, 1, 2, 3, \cdots, 39$ 时的值都是素数．斯塔克(H.M.Stark)曾证明②，当 $A > 41$ 时不存在那样的二次型 $x^2 + x + A$，它对于 x 的 $A-1$ 个相邻的值皆表示素数．

任给的一个数 N，如果能够不必检查每个小于 $\sqrt{N}$ 的素数 [60]
是否 N 的除数就断定 N 是否素数，那显然是令人向往的．我将叙述两种判别法．

威尔逊先生(J. Wilson)(1770)发现并经拉格朗日(Lagrange)证明(1773)：当且仅当 $(N-1)!+1$ 可被 N 整除时，N 为素数．例如，$(7-1)!+1 = 721$ 可被 7 整除，但 $(9-1)!+1 = 40321$ 不能被 9 整除．威尔逊定理宁可说是对素性的一个理论上的而不是实际上的判别，因为，如果 N 很大以致不易弄清它是否一个素数，那么要肯定 $(N-1)!+1$ 是否能被 N 整除将比检查每一个小于 $\sqrt{N}$ 的素数是否 N 的一个因子更为麻烦．

费马(Fermat)发现(1640)并经欧拉证明(1736)，若 p 为素

---

① Nouveaux Mèmoires de l'Académie royale des Sciences, Berlin, 1772, p.36.

② Michigan Mathematical Journal, 1967, Vol. XIV, pp.1—27.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

数且不能整除 a,则 $a^{p-1}-1$ 可被 p 整除.中国人早在公元前500 年就已知道 $a=2$ 的情况;他们还陈述过逆命题:若 N 能整除 $2^{N-1}-1$,则 N 为一个素数.这个命题于 1680 年又被莱布尼茨重新发现并且"证明"了.然而它是错误的,因为当 $N=341=11\times 31$ 以及无穷多个别的 N 值时它都不成立.现代的素性检验是以吕卡斯(E. Lucas)的定理(费马定理的逆定理)①为依据的.此定理谓:若 a^x-1 当 $x=N-1$ 时可被 N 整除而当 x 为 $N-1$ 的一个真因子又不能被 N 整除,则 N 为一个素数.在真正的现代检验出世之前,对于这个逆定理中的条件与结论的修改都是必需的②.

大约在 1930 年,D·H·雷默(他的父亲构制成了第一个真正重要的因子表与素数表③)发明一种光电数字筛,它能够以惊人的速率把大的数字分解因子.其后的四十年中,他和他的助手们
[61] 继而把光电筛改进为电子筛④,其运算速度为每秒种一百万次,七倍于 IBM7090 的速度.

要一个人给下述命题迅速作出证明是很有趣的:每两个相邻的奇素数之和等于三个大于1的整数的乘积.例如,7 + 11 =

---

① Théorie des Nombres, Paris, 1891, pp. 423,441. 关于费马定理的一个有趣的讨论,见 E·T·贝尔(E.T.Bell)的 Numerology, Baltimore, 1933, pp. 182—185.

② 参看 Bulletin of the American Mathematical Society, 1927, Vol. XXXIII, pp. 327—340.

③ D.N. Lehmer, Factor Tables for the First ten Millions, Washington, 1909; List of Prime Numbers from 1 to 10 006 721, Washington, 1914. 后一本书有一篇特别引人入胜的引言.

④ J.D. Brillhard and J. Selfridge, Mathematics of Computation, 1967, Vol. XXI, pp. 87—96. 关于 Viggo Brun, Atle Selberg 等人的筛理论的发展的一篇易读的报告,参看 H. Halberstam 与 K.F. Roth, Sequences, 1966, Vol. Ⅰ, Chapter Ⅳ.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$2\times3\times3$, $11+13=2\times3\times4$. 初看这似乎很难，但实际是很容易的.

素 数 定 理

欧拉(1737)以优美的形式表出了算术的基本定理(此定理谓每个自然数皆有唯一的因子分解式)：

$$\sum_{n=1}^{\infty} n^{-s} = \prod_p (1 + p^{-s} + p^{-2s} + \cdots) = \prod_p (1 - p^{-s})^{-1},$$

其中求积号遍及一切素数.

用 $\pi(X)$ 表示不超过 X 的素数的个数，则 $\pi(2)=1$, $\pi(10)=4$, $\pi(100)=25$, 等等. 在检视了 400 000 以内的素数表之后，勒让德(A.M.Legendre)(1808)断言，当 X 很大时，$\pi(X)$ 的近似值为

$$X/(\log X - B),$$

其中 B 为接近 1 的一个常数. 阿贝尔(N.H.Abel)(在 1823 年的一封信中)称这个定理为"在整个数学中最值得注意的". 高斯(1849 年)独立地提出，若 X 很大而 x 相对地很小，则介于 X 和 $X+x$(或 $X-x$ 和 X)之间的素数的个数大约是 $x/(\log X)$，所以 $\pi(X)$ 大约等于

$$\int_2^x \frac{dt}{\log t}.$$

这两个近似式都是著名的素数定理的推论，此定理称 $\pi(X)$ 与 $X/(\log X)$ 的比当 X 趋于无穷时趋于 1. 这是 1896 年分别由阿达玛(J.Hadamard)与瓦莱·普桑(de la Valleé Poussin)[1]独立证明 [62]
的. 二十五年后，赛尔伯格(A. Selberg)与爱尔特希(P. Erdös)[2]发

---

① Jaques Hadamard, Bulletin de la Société mathematique de France, 1896, Vol. XXIV, pp. 199—220; C.J. de la Vallée Poussin, Annales de la Société Scientifique de Bruxelles, 1896, Vol. XX. pp. 183—256.

② Annals of Mathematics, 1949, series 2, Vol.L, pp.305—315.

我们必须知道，而且我们必将知道

明了素数定理的一个初等的(但是相当长的)证明.他们的证明是惊人的,因为迄今所有的证明都主要依赖于复变函数论中的技巧,特别是依赖于把函数 $\pi(X)$ 的性态与勘查黎曼 ζ 函数

$$\zeta(S)=\sum_{n=1}^{\infty}n^{-s}$$

在复 S 平面上的零点位置的问题关联起来的想法[可追溯到黎曼(B. Riemann)①].事实上,这个似乎难以对付的黎曼假说断言 $\zeta(S)$ 的一切非实数零点都聚集于直线 $\mathrm{Re}(S)=\frac{1}{2}$ 上.由此,用较方便的"对数积分"

$$\mathrm{li}X=\lim_{\varepsilon\to+0}\left(\int_0^{1-\varepsilon}+\int_{1+\varepsilon}^{X}\right)\frac{\mathrm{d}t}{\log t}$$

代替 $X/(\log X)$,则可推出

$$|\mathrm{li}X-\pi(X)|<cX^{1/2}\log X,$$

其中 c 为某一正的常数.这是比任何已知的强化了的素数定理还要强得多的论断.②

至于数字的证实,已经计算出

$$\mathrm{li}10^9=50\ 849\ 235,\quad \pi(10^9)=50\ 849\ 234.$$

(前者是经过四舍五入所得的整数;后者是精确数字.)虽然在每个已知的情况皆有 $x>\pi(X)$,可是李特尔伍德(J.E.Littlewood)证明了(1914 年):如果让 X 不断增大,那么终于会达到一个 X
[63] 值使不等号颠倒过来;而且这种颠倒会发生无穷多次!

德·波利尼亚克(A.de Polignac)③曾猜想:每个偶数皆可表

---

① Monatsberichte der Preussichen Akademie der Wissenschaften, 1859, pp. 671—680.

② A. E. Ingham, The Distribution of Prime Numbers, Cambridge, 1932, p. 83.

③ Nouvelles Annales de Math., 1849, Vol. VIII, p.428.

http://maths352.bokee.com

示为两个相邻素数的差，且这种表示有无穷多个. 取偶数为 2，则此猜想就是说有无穷多对素数，它们是相邻的奇数. 例如 5，7；11，13；17，19；29，31；41，43；59，61；71，73. 这个猜想既未获证明也未被推翻. 人们发现，在 $10^{12} \pm 10^4$ 这个区间内有 36 对这种实例. 大得惊人的例子是素数偶

$$9 \times 2^{211} \pm 1,$$

其中较小的一个是雷默发现的，较大的一个是鲁宾逊（R.M. Robinson）①发现的.

相当容易证明：当 X 无限增大时，一切小于 X 的素数之和也无限增大. 然而，如果只考虑那些相差为 2 的素数偶，那么当 X 无限增大时，它们的倒数之和却是有界的. 这个结论是布伦（V.Brun）的，它表明相差为 2 的素数偶并不"太多".

与此有些相仿的猜想是哥德巴赫（Goldbach）定理：每个大于 4 的偶数可以表示为两个奇素数之和. 直到 10000 的偶数与少量很大的偶数都经过了验证. 维诺格拉多夫（L.A. Vinogradoff）②于 1937 年证明了：每个充分大的奇数是三个素数的和. 埃斯特曼（T.Estermann）③发现几乎一切偶数都是两个素数的和.

默 森 数

人们在 1644 年出版的默森（Mersenne）所著"Cogitata Physico－Mathematica"④里发现关于形为 $2^p - 1$ 的数之为素数或合数

① R.M. Robinson, Proceedings of the American Mathematical Society, 1958, Vol. Ⅸ. p. 674.

② I.M. Vinogradov, The Method of Trigonometric Sums in the Theory of Numbers, London, 1954, p.167.

③ Proceedings of the London Mathematical Society, ser.2, 1938, Vol. XLIV, pp. 307—314.

④ 《物理学与数学的深思》.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



[64] 的一个奇妙的论断(但是不完全正确).在该著作的序言里有一段关于完全数的论述,其中说道:在不大于 257 的 p 值中,使 2^p-1 为素数者只有 2,3,5,7,13,17,19,31,67,127 与 257.这个论断起初似乎不大受人重视,因为它包含着五个错误.1883 年佩尔武申(I.M. Pervusin)发现 $2^{61}-1$ 是个素数①.1903 年 F·N·科尔(F.N.Cole)得到因子分解

$$2^{67}-1=193707721\times761838257287.$$

波尔斯(R.E.Powers)②相继于 1911 年和 1914 年发现 $2^{89}-1$ 和 $2^{107}-1$ 都是素数.克拉依切克(M.Kraïtchik)③于 1922 年发现 $2^{257}-1$ 是合数.

现代的办法是 1877 年吕卡斯④奠定的,并且他还曾用以证明默森的断言:$2^{127}-1$(= 170 141 183 460 469 231 731 687 303 715 884 105 727)是素数.在而后的七十五年中(确切地说,直到 1952 年元月 30 日),这是最大的已知素数.雷默⑤于 1931 年将吕卡的方法改进成如下的单一判断:

$2^p-1(p>2)$当且仅当它整除 v_{p-1}时才是素数,这里 $v_1=4$ 且 $v_{n+1}=v_n{}^2-2$.

作为例证,我们注意 2^3-1 整除 $v_2=14$,2^4-1 不能整除 $v_3=194$,2^5-1 整除 $v_4=37634$.

这个强有力的判断已经借助于计算机去检验所有 $p<20000$的默森数2^p-1.结果是这些默森数中只有24个是素数,

① R.C.Archibald, Scripta Mathematica, 1935, Vol. Ⅲ, p.117.

② American Mathematical Monthly, 1911, Vol. XVIII, pp. 195—197;Proceedings of the London Mathematical Society, ser. 2, 1919, Vol. Ⅻ, p.39.

③ 参看 Sphinx, 1931, p. 31.

④ American Journal of Mathematics, 1878, Vol. Ⅰ, p.316.

⑤ Sphinx, 1931, pp. 32, 164.

我们必须知道,而且我们必将知道

http://maths352.bokee.com



即①当 p 取下列各值时:

2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2203,2281,3217,4253,4423,9689,9941,11213,19937. [65]

塔克曼用 IBM360/91 计算机(运行刚刚不到四十分钟)证明了 v_{19936} 可被 $2^{19937}-1$ 整除.这第二十四个默森素数有 6002 位.

对于中等 p 值(实即一切 $p<20\ 000$)所给的默森数,一切小于 2^{34} 的素因子都已经被找到了.下边是几个惊人的因子分解:

$2^{101}-1=7\ 432\ 339\ 208\ 719\times 341\ 117\ 531\ 003\ 194\ 129$

[约翰逊(C.O.Johnson)],

$2^{103}-1=2\ 550\ 183\ 799\times 3\ 976\ 656\ 429\ 941\ 438\ 590\ 393$

[布里尔哈德(Brillhart)],

$2^{109}-1=745\ 988\ 807\times 870\ 035\ 986\ 098\ 720\ 987\ 332\ 873$

[伽巴德(Gabard)],

$2^{113}-1=3\ 391\times 23\ 279\times 65\ 993\times 1868\ 569$
$\times 1\ 066\ 818\ 132\ 868\ 207$ (雷默).

布里尔哈德曾证明 $(2^{131}-1)/263$ 是素数.

吉利斯(Gillis)曾猜想:小于 X 的默森素数的个数大约是

$$\frac{2\log\log X}{\log 2}.$$

完　全　数

完全数的理论直接依赖于默森数的理论.若一个数等于它的所有真因子的和,则称此数为完全的.例如 6 与 28 都是完全

---

① 这些 p 值中,521 与 607 是雷默和 R·M·鲁宾逊发现的;1 279,2 203 与 2 281 是雷默发现的;3 217 是安德森(A. Anderson)和里塞尔(W. Riesel)发现的;4 253 与 4 423 是胡尔维茨发现的;9 689,9 941 与 11 213 是吉利斯(D.B.Gillies)发现的(Mathematics of Computation, 1964, Vol. XVIII, pp. 93—97);19 937 是塔克曼(B.Tuckerman)发现的(Notices of the American Mathematical Society, 1971, Vol. XVIII, p.608).

我们必须知道，而且我们必将知道

http://maths352.bokee.com

数，因为 $6=1+2+3$，$28=1+2+4+7+14$. 神秘主义者对这两个数特别有兴趣，因为创造世界用了 6 天，阴历的一个月有 28 天.

欧几里得证明了凡 2^p-1 为素数时，$2^{p-1}(2^p-1)$ 都是完全数. 因为对 $2^{p-1}(2^p-1)$ 来说其因子（包括它自身）是 2^n 与 $2^n(2^p-1)$，$n=0,1,\cdots,p-1$，并且我们知道 $1+2+2^2+\cdots+2^{p-1}=2^p-1$.

欧拉证明了：这个公式包括了一切偶的完全数. 下边的简化
[66] 证明是迪克森（L.E.Dickson）①给出的. 设 2^nq 为完全数，q 是奇数且 $n>0$. 于是 $2^{n+1}q=(2^{n+1}-1)S$，这里 S 是 q 的一切因子的和. 所以 $S=q+d$，这里 $d=q/(2^{n+1}-1)$. 因此，d 是 q 的一个因子，从而可知 q 与 d 是 q 仅有的因子. 所以 $d=1$ 而 $q=2^{n+1}-1$ 是一个素数.

当 $p=2,3,5,7,13,17,19,31$ 时得到默森素数 3，7，31，127，8 191，131 071，524 827，2 147 483 647 与完全数 6，28，496，8 128，33 550 336，8 589 869 056，137 438 691 328，2 305 843 008 139 952 128. 容易证明：一个偶完全数的末两位数码必是 28 或者 6 且（除了 6 自身）6 的前一位是个奇数. 还有，每个偶完全数除了 6 之外与 1 关于模 9 同余.

---

① L.E.Dickson, American Mathematical Monthly, 1911, Vol. XVIII, p. 109. 也可参看他的 History of the Theory of Numbers, Vol. Ⅰ, Washington, 1919. 有理由相信，每个完全数都是偶数. 无论如何，小于 10^{36} 的奇数没有一个是完全数，这是由塔克曼证明了的（Notices of the American Mathematical Society, 1968, Vol. XV, p.226）. 西尔维斯特（J.J.Sylvester）猜想并由格拉德施坦（I.S.Gradstein）证明了（1925 年的一篇俄语论文中）：如果有一个奇的完全数存在，那么它必须有至少六个不同的素因子. 一个奇的完全数的存在蕴含着有两个或更多的奇数存在，它们的倒数之和为 1. 寻求这样的奇数似乎比寻求一个奇的完全数较可能成功.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

费 马 数

费马(Fermat)以大量的新命题丰富了数学.除了一个例外,所有这些命题都已被证明或者被相信是正确的.这个例外就是他的二的乘幂定理.这定理说,一切形状为 2^m+1 的数其 $m=2^n$ 者皆为素数①.可是他又补充说,虽然他相信这个命题是正确的,但是他未能作出实质性的证明.

可以证明,若 m 不是 2 的一个乘幂,则 2^m+1 为合数.但是,当然不能由此推论若 m 是 2 的一个乘幂,如 2^n,则 2^m+1 就是一个素数.事实上,这定理是不成立的.欧拉②于 1732 年证明了:若 [67]
$n=5$,则公式给出的数是 4 294 967 297,它等于 $641\times 6\,700\,417$.

让我们定义

$$F_n=2^{2^n}+1.$$

于是 $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65\ 537$.本内特(G. T. Bennett)③曾说明怎样不用实行除法运算就能证明 F_5 可被 641 整除:数

$$641=5^4+2^4=2^7\cdot 5+1$$

既能整除 $2^{28}(5^4+2^4)$ 又能整除 $(2^7\cdot 5)^4-1$,所以也能整除它们的差,这差正是 $2^{32}+1$.

借助于二次剩余的高斯理论,可证 $F_n(n>1)$ 的任一素因

① 1640 年 10 月 18 日的信,Opera, Toulouse, 1679, p. 162;或布拉辛尼(Brassinne)的 Précis, p. 143.

② Commentarii Academiae Scientiarum Petropolitanae, Leningrad, 1738, Vol. Ⅵ, p. 104;又见 Novi Comm. Acad. Sci. Petrop., Leningrad, 1764, Vol. Ⅸ, p. 101;或 Commentationes Arithmeticae Collectae, Leningrad, 1849, Vol. Ⅰ, pp. 2, 357.

③ 比较哈代(G. H. Hardy)与赖特(E. M. Wright)著, An Introduction to the Theory of Numbers, Oxford, 1954, p. 14.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

子必具形式 $2^{n+2}\cdot k+1$，这里 k 是一个整数．例如

$$F_5=(2^7\cdot 5+1)(2^7\cdot 52347+1),$$

以及 1880 年兰德里（F．Landry）看出的

$$F_6=(2^8\cdot 1\,071+1)(2^8\cdot 262\,814\,145\,745+1).$$

1909 年莫尔黑德（J．C．Morehead）与韦斯顿（A．E．Western）证明了 F_7 与 F_8 都是合数．利用下边的判据很容易检验这个结论．

$F_n(n>0)$ 当且仅当它整除 $3^{(F_n-1)/2}+1$ 时为素数．

发现了 F_7 与 F_8 为合数之后的六十年中，一直未能找到两者之中任一个的因子，虽然证明了 F_7 是两个两个素数的乘积．1970 年，莫里森（M．A．Morrison）与布里尔哈德（J．D．Brillhart）①终于找到了这两个素数，从此我们才知道

$$F_7=(2^9\cdot 116\,503\,103\,764\,643+1)$$

68 $$\times(2^9\cdot 11\,141\,971\,095\,088\,142\,685+1).$$

当 $n=9,10,11,12,15,16,18,23,36,38,39,55,58,63,73,77,81,117,125,144,150,207,226,228,250,267,268,284,316,452,1\,945$ 时已经知道 F_n 的至少一个因子．详细情况（包括发现者和发现日期）已由 R·M·鲁宾逊②制成简洁的一览表，他还指出一切小于 2^{35}的因子也都已经知道了．帕克森（G．A．Paxson）证实了（计算时间 $6\frac{1}{4}$小时稍强）F_{13}为合数，塞尔弗里奇（J．L．Selfridge）与胡尔维茨证实了 F_{14}为合数．F_{1945}是迄今研究过的最大数字之一．要把它明显地写出来是一件不可能的事，因为它的位数远远超过宇宙中的粒子数（据已故的爱丁顿（A．S．Eddington）计算，那是 51×2^{260}）．

---

① Bulletin of the American Mathematical Society，1971．Vol．LXXVII，p．264．

② Proceedings of the American Mathematical Society，1958．Vol．Ⅸ，p．679．

我们必须知道，而且我们必将知道

http://maths352.bokee.com



所有这些结果都支持这样一个猜想：当 $n>4$ 时 F_n 都是合数.

费马最后定理

我现在转到费马提出而迄今尚未得到证明的论断.这个定理有时称为费马的最后定理，其大意①谓：若 n 为大于 2 的整数，则方程 $x^n+y^n=z^n(xyz\neq 0)$ 没有整数解.这个定理享有非常的盛誉，因为既没有理由怀疑它的正确性，又从来没有人能给出一般的证明②.

似乎费马首先对 $n=3$③的情况发现了它的真实性，然后是 $n=4$ 的情况.他的对前一种情况的证明丢失了，现存的是他的对后一种情况的证明④和欧拉⑤给出的对 $n=3$ 的情况的类似 [69]

---

① 费马的文章可以在他的出版物 Diophantus 里找到，Toulouse，1670，bk. Ⅱ，qu.8，p.61；或参看布拉辛尼的 Présis，Paris，1853，p.53.参考书刊目录见迪克森（L. E. Dickson），History of the Theory of Numbers，Washington，1920，Vol，Ⅱ，Ch.26；又见莫德尔（L·J·Mordell），Fermat's Last Theorem，Cambridge，1921，在克莱茵（F. Klein）等人的 Famous Problems and Other Monographs，New York，1955，书中有转载.莫德尔称 $x^n+y^n=z^n$ 为“一切丢番图（Diophantine）方程中最著名的方程”.

② 这个具有 350 多年历史的世界难题已由英国数学家怀尔斯（A. Wiles）于 1994 年解决.论文发表于《数学年刊》（Annals of Mathematics）的 142 卷第 3 期（1995 年 5 月号）上.详情请参见本译丛中《数学：新的黄金时代》的第 8 章.《费马大定理》（西蒙·辛格著，薛密译，上海译文出版社，1998 年版）对这项彪炳青史的成就作了纪实文学式的描述.——译者注

③ 见我的 History of Mathematics，4th. ed.，Dover reprint，New York，1960，Chapter XV 中所引费马的一封信.

④ 费马的 Diophantus，p.339 上的注；或布拉辛尼的 Précis，p.127.

⑤ 欧拉的 Algebra（英译本 1797），Vol. Ⅱ. Chap. XV，p.247；有一点被欧拉疏忽了，但这点遗漏是可以补充上的.欲看当 $n=4$ 与 $n=3$ 两种情况的完全讨论，可参考 Hardy and Wright，An Introduction to the Theory of Numbers，pp.191—194.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的证明概要.这些证明依赖于论证:如果能够找到适合此方程的 x,y,z 的一组整数值,那么就能够再找到另一组较小的整数值,它们也适合此方程.这样推下去,我们最终证明此方程必须被显然不适合它的一组值适合.所以它不可能有整数解.这个方法不能用于一般的情况.

费马的一般定理的发现较晚.可以在每个整数都有唯一的素因子分解的假定下给出一个证明.虽说这个假定对于每个"有理"整数是成立的,但是对于每个"代数"整数这个假定就不对了.一个代数整数就是多项式方程

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

的一个根,其中系数 a_i 都是有理整数.例如,在代数整数 $a + b\sqrt{10}$(其中 a 与 b 皆为有理整数)的环里,数 6 有两种不同的素因子分解:

$$6 = 2 \times 3 = (4 - \sqrt{10})(4 + \sqrt{10}).$$

相仿地,当 n 取某些值时,费马的方程导致一些式子,它们都有多种不同的因子分解.费马的论证可能就是以上述错误的假设为依据的,但这只是一个无根据的猜测.不管怎样,他明确地宣称过他有一个有效的证明——demonstratio mirabilis sane(完美的论证).凡是他陈述的论题中证明过的定理,过后没有人能指出哪一条是不成立的,这一点他很持重.当他在他的著作中提出一个没有把握的断言时(例如,说 F_n 是素数)尤其如此,他当时
[70] 就声明他未能作出一个满意的证明.

必须记住,费马是当之无愧的第一流的数学家,他对数论做过特殊的研究.这个课题本身是特别有趣而美妙的,但它的结论没有什么实用上的重要性,因而长期以来只有很少几个数学家去研究它.这说明为什么费马宣布的某些简单结论过了一个多世纪才得到证明,而他晚年建立的定理的证明有着高度的困难也就不奇怪了.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

1823 年勒让德①得到 $n=5$ 时的证明；1832 年狄利克雷（L. Dirichlet）②给出 $n=14$ 时的证明；1840 年拉梅（G. Lamé）与勒贝格（H. Lebesgue）③给出 $n=7$ 时的证明.

要证明 $n>4$ 时的命题，显然只需研究 n 为素数的那些情况就够了. 1849 年库默尔（E. E. Kummer）④证明了一切"正则"素数的情况.（素数 p 若不能整除伯努利数⑤ $B_1, B_2, \cdots, B_{\frac{1}{2}(p-3)}$ 的分子则称之正则的.）库麦尔发现，小于 164 的"非正则"素数只有 37，59，67，101，103，131，149，157. 塞尔弗里奇和波洛克（B. W. Pollock）利用 SWAC 高速计算机已经找到了小于 25 000 的一切非正则素数并逐个进行了检验，结论是：定理当 $n<25\ 000$ 时成立. 其他判别法也建立了，例如，威斐礼奇（A. Wieferich）⑥曾证明：若方 [71]
程有与 n 互素（n 为奇素数）的整数解，则 $2^{n-1}-1$ 可被 n^2 整除. 这个受限制的问题已经分别由罗瑟（J. B. Rosser）和雷默⑦推进到了 $n=41\ 000\ 000$ 与 $250\ 000\ 000$. 很久以前就设立了十万马克的奖

① 复载于他的 Théorie des Nombres 里，Paris，1830. Vol. Ⅱ，pp. 361—368；又见 pp.5，6.

② Crelle's Journal，1832，Vol. Ⅸ，pp. 390—393.

③ Liouville's Journal，1841，Vol. Ⅴ，pp. 195—215，276—279，348—349.

④ 库麦尔报告的参考资料见于 H. S. Vandiver，Transactions of the American Mathematical Society，1929，Vol. XXXI，pp.613—642.

⑤ 伯努利数出现在级数

$$\frac{x}{2}\cot\frac{x}{2}=1-\frac{B_1}{2!}x^2-\frac{B_2}{4!}x^4-\frac{B_3}{6!}x^6-\cdots$$

里，前八个数值是 $\frac{1}{6}, \frac{1}{30}, \frac{1}{42}, \frac{1}{30}, \frac{5}{66}, \frac{691}{2730}, \frac{7}{6}, \frac{3617}{510}$.

⑥ Crelle's Journal，1909，Vol. CXXXVI，pp.293—302.

⑦ Bulletin of the American Mathematical Society，1941，Vol. XLVII，p.142.

我们必须知道，而且我们必将知道

金①,要求在 2007 年之前作出一个一般的证明.

尽管费马问题仍然没有解决,它对数论是非常重要的,因为许多现代方法都是联系着它而发展起来的,而且与之有关的许多理论的出现恐怕要比证明这定理本身更为重要.费马是怎样得到他的结果的,自然曾有过许多臆测.现存的他的那些证明所涉不外乎初等几何与代数,甚至他的有些论证里连任何符号都不用.这使有些数学家认为除了初等数学以外费马什么都没用到.事情也可能是那样,不过,下边的注记(我相信一般人是不知道的)表明颇为不然.他曾向英国数学家们提出过一个问题:证明方程 $x^2+2=y^3$ 仅有一组整数解.这解显然是 $x=5,y=3$.关于这个问题他有一个注记②,大意说,要找有理分数解是不难的,但是他已经发现了一个全然新颖的方法——sane pulcherrima et subtilissima(完善而最精致)——有了它,他能求该问题的整数解.他本打算写一篇他在数论方面研究工作的综合性文章③,但是它从未完成,因而关于他的分析方法后人所知甚少.我冒昧添一句私下的猜疑,在他的研究中,连分式可能起着重要的作用.作为这一猜测的佐证,我可以指出,他的某些奥妙的结
[72] 论是可以利用连分式的性质比较容易得到的,例如定理:形状为 $4n+1$ 的素数可以表示为两个数的平方和④.

伽 罗 瓦 域

在实数域、有理数域和复数域里都成立的加法和乘法的熟

---

① L'Intermédiaire des Mathématiciens, Vol. XV, pp.217—218.

② Fermat, Diophantus, bk. Ⅵ, prop. 19, p. 320;或 Brassinne Précis, p.122.

③ Fermat, Diophantus, bk. Ⅳ, prop. 31, p. 181;或 Brassinne, Précis, p. 82.

④ Fermat, Diophantus, bk. Ⅲ, prop. 22, p. 127;或 Brassinne, Précis, p. 65.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

知性质（如结合律、分配律、交换律，以及可用非零元素除），在某些元素个数有限的域里也成立. 可以证明①：这个有限的数 q 必为某一素数的乘幂，如，$q=p^n$，这里 p 为一素数，n 为一正整数. 对于每个素幂 q 恰有一个域，记为 GF(q)，读作一个伽罗瓦域——以伽罗瓦（Evariste—Galois）（1811—1832）命名的域. 他的光辉的业绩在一次决斗中夭折了②. 特殊地，GF(p)是关于模 p 的剩余类的域，其 p 个元素记为 $0,1,\cdots,p-1$，这里（约定）0 的意思是 p 的一切整倍数的集合，1 的意思是当用 p 除时余数为 1 的一切整数的集合，如此等等. 当然，完全可以把 $p-1$ 叫做 -1. 例如，由于 $641=1+2^7\cdot 5=2^4+5^4$，下边的等式在 GF(641)里成立：

$$2^7\cdot 5=-1,\quad 2^4=-5^4,$$

$$2^7=-\frac{1}{5},\quad 2^8=-\frac{2}{5},\quad 2^{32}=\left(-\frac{2}{5}\right)^4=\frac{2^4}{5^4}=-1.$$

这就是克拉伊切克对于 641 能整除 $2^{32}+1$ 的证明③. 论断"在 GF(p)里 $a=b$"的意义与

$$a\equiv b\pmod{p}$$

一样（即"a 和 b 关于模 p 同余"），也就是说，$a-b$ 可被 p 整除.

记号 $a\equiv b\pmod{m}$ 也用于当 m 为合数时，不过这时的剩余类仅构成一个环而不构成一个域. 例如，在以 4 为模的剩余类 [73]
里，$2\times 2\equiv 0$，而 0 没有逆元. 所以，虽然这个环有 4 个元素，但是它和域 GF(4)很不相同. 为了强调它们的区别，通常把记号 GF(4)推广为 GF(2^2).

---

① Garret Birkhoff and Saunders Maclane, A Survey of Modern Algebra (3rd, ed.), New York, 1965, p. 413. 又见 L. E. Dickson, History of the Theory of Numbers, Vol. I, Washington, 1919, p. viii.

② Leopold Infeld, Whom the Gods Love, New York, 1948.

③ M. Kraïtchik, Théorie des Nombres, Vol. II, Paris, 1926, p. 221.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

当 $n>1$ 时，$GF(p^n)$ 皆可表示为系数属于 $GF(p)$ 的多项式等价类的域．两个这样的多项式称为是等价的，若它们的差可被一个特定的不可约（或“素”）n 次多项式整除．于是，$GF(p^n)$ 的 p^n 个元素中每一个都可以表示为一个次数低于 n 的多项式．（尽管一般地有几个多项式，它们都生成同一个域 $GF(p^n)$．）

采用分离系数法常常是方便的，例如把 x^3+2x+1 写成 1 021（若 x 表示 10，则此数具有通常的意义）．当取 1 021 为 $GF(3^3)$ 的模时，一个典型的加法例子是（先用多项式表示，后用分离系数法）

$$\begin{array}{r} x^2+2x+1 \\ 2x+2 \\ \hline x^2+x \end{array} \qquad \begin{array}{r} 1\ 2\ 1 \\ 2\ 2 \\ \hline 1\ 1\ 0 \end{array}$$

一个典型的乘法例子是

$$\begin{array}{r} x^2+2x+1 \\ x \\ \hline x^3+2x^2+x \\ x^3+2x+1 \\ \hline 2x^2+2x+2 \end{array} \qquad \begin{array}{r} 1\ 2\ 1 \\ 1\ 0 \\ \hline 1\ 2\ 1\ 0 \\ 1\ 0\ 2\ 1 \\ \hline 2\ 2\ 2 \end{array}$$

（最后一步是减去模 1021．）众知，每个非零元素都是某一适当的“素元”的一个幂．例如，在上述的 $GF(3^3)$ 的表示中，每个非零元素都是 10 或 x 的一个幂①：

$$x^0=1, x^1=10, x^2=100, x^3=1000=12, \cdots,$$

[74]

$$x^{13}=2, \cdots, x^{26}=1.$$

元素 $1, x^2, x^4, \cdots$ 都是平方，而（p 为奇数）$x^3, x^5, \cdots$ 都是非平方．约定 $x^\infty=0$，则零元素可以被包括进去，它较好地符合法则 $x^a \cdot x^b = x^{a+b}$．

在任一域里，特别是在一个有限域里，研究诸如

① 第一个“…”依次表示 120，212，111，122，202，11，110，112，102．——译者注

我们必须知道，而且我们必将知道

$$ay^l + bz^m + c = 0$$

之类的代数方程的解都是很有趣的问题.高斯①就已经知道当 $(l, m) = (2,2), (3,3), (4,4), (2,4)$ 时解的个数的公式.然而,对一般问题的最深入的探讨的出现要晚得多,那是韦伊(A. Weil)②的灵机所获(藉助于代数函数域的理论).类似于黎曼对有理域所做的情况③,可以对这样的方程所确定的函数域伴随一个 ζ 函数,并且完全与古典的情况相仿地提出一个勘查其零点的假设.韦伊的重大成就是给黎曼假设的所谓"有限类比"提供一个证明,它不仅在数论里而且在有限域上的代数几何学里引起了深刻的进展. [75]

---

① C.F.Gauss, Werke, 1900, Vol. Ⅰ, pp. 445—449.

② Sur les courbes algébriques et les variétés qui s'en déduisent, Paris, 1948.

③ 关于这个理论的细节,参看 M. Eichler, Algebraic Numbers and Functions, New York, 1966 (由 1963 年德文版译成), § 5.1.

第3章 几何趣谈

在这一章和下一章里我打算列举一些几何问题、难题和游戏，在讨论它们时用不着多少代数或算术.这一章的大部分都是些形式命题;下一章的内容是各种游戏的介绍.

按照我在序言里给自己定下的原则，我排除了涉及高等数学的定理的详细讨论.此外(除了一两个例外)，我还排除了那些仅仅依赖于当图形的相对位置改变时人们的眼睛对其尺寸产生错觉的几何悖论的任何陈述.这种表观上的骗局与思维推理能力无涉，而是建立在视觉的错误判断上，我认为此类悖论不应归入数学的范畴里.

几何谬论

大多数受过教育的英国人对于几何学里和欧几里得的名字联系着的许多逻辑命题都是熟悉的，但是作为对那些命题的补充，原来还有一些习题，这个情况就不那么普遍为人所知了.欧几里得把那些习题配置成三个系列，两个系列包含的是比较容易的定理或问题，第三个是由一些几何谬论组成的，要求学生找出其中的错处.

欧几里得收集的谬论已失传了.关于那些错误推理或结论
[76] 的性质，传统的著述中也没有保存下来任何记载.不过，作为此类问题的例示，我给出个别典范，它们导致显然是不可能的结论.任何人初次见到时恐怕都觉得很有趣.我把错误的揭露留给

我们必须知道，而且我们必将知道

http://maths352.bokee.com

读者去发挥自己的才能.

第一个谬论① 证明直角等于钝角.

令 $ABCD$ 为一矩形. 如下图所示，由 A 向矩形外引直线 AE，其长等于 AB 或 DC，并与 AB 成锐角. 因 CB 与 CE 不平行，它们的中垂线 HO 与 KO 必相交于一点，记为 O. 连 OA，OE，OC、OD.

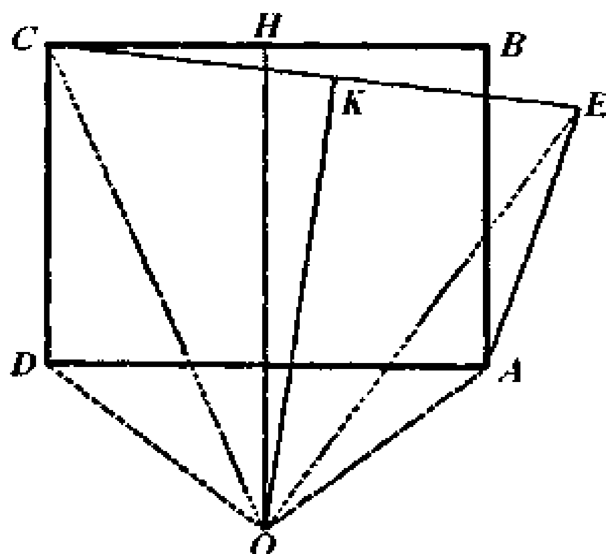


图 3.1

显然，三角形 ODC 与 OAE 全等. 因为 KO 等分 CE 且和它垂直，所以 $OC = OE$. 相仿地，因 HO 等分 CB 与 DA 且垂直于它们，故 $OD = OA$. 还有，由作图知 $DC = AE$. 所以三角形 ODC 的三个边分别等于三角形 OAE 的三个边. 因此，据《几何原本》
Ⅰ.8，这两个三角形全等；于是角 ODC 等于角 OAE. [77]

再者，因 HO 等分 DA 且垂直于 DA，故角 ODA 等于角 OAD.

---

① 我相信这个谬论和下边第四个谬论都是首先载于本书中. 它们特别引起了 C. L. 道奇森（C. L. Dodgson）先生的兴趣. 参看 Lewis Carroll Picture Book, London, 1899, pp. 264, 266, 它们以我最初给出的形式出现于其中.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

所以角 ADC(它是 ODC 与 ODA 的差)等于角 DAE(它是 OAE 与 OAD 的差).但 ADC 是一个直角,而 DAE 必然大于一个直角.所以,结果是不可能的.

第二个谬论① 证明线段的部分等于全体.

令 ABC 为一三角形.为确切计,设它是一个不等边三角形,且角 B 为锐角、角 A 大于角 C.由 A 作 AD,使角 BAD 等于角 C,并与 BC 交于 D.由 A 作 AE,垂直于 BC.

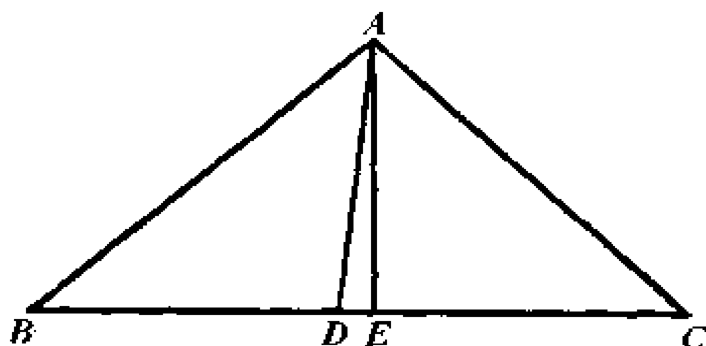


图 3.2

三角形 ABC 与 ABD 的相当角相等,所以

$$\triangle ABC : \triangle ABD = AC^2 : AD^2.$$

又,三角形 ABC 与 ABD 同高(高度为 AE),故

$$\triangle ABC : \triangle ABD = BC : BD.$$

$$\therefore \quad AC^2 : AD^2 = BC : BD.$$

$$\therefore \quad \frac{AC^2}{BC} = \frac{AD^2}{BD}.$$

再利用余弦定理改写此等式中的分子,得

[78]

$$\frac{AB^2 + BC^2 - 2BC \cdot AB}{BC} = \frac{AB^2 + BD^2 - 2BD \cdot AB}{BD}.$$

$$\therefore \quad \frac{AB^2}{BC} + BC - 2AB = \frac{AB^2}{BD} + BD - 2AB.$$

① 参看科克兹(M. Coccoz)的一个注记,载于 L'Illustration, Paris, Jan. 12, 1895.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

$$\therefore \quad \frac{AB^2}{BC} - BD = \frac{AB^2}{BD} - BC.$$

$$\therefore \quad \frac{AB^2 - BC \cdot BD}{BC} = \frac{AB^2 - BC \cdot BD}{BD}.$$

$$\therefore \quad BC = BD,$$

这个结果是不可能的.

第三个谬论① 证明任一三角形的两边长之和等于第三边长.

令 ABC 为一三角形.以 AB 与 BC 为两边作平行四边形.将 AB 分为 $n+1$ 等份,通过分点作 n 条直线平行于 BC.相仿地,将 BC 也分为 $n+1$ 等份,并通过分点作 n 条直线平行于 AB.于是,平行四边形 $ABCD$ 被分成 $(n+1)^2$ 个相等而且相似的小平行四边形.

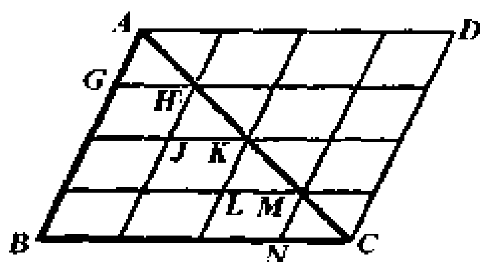


图 3.3

图中画的是 n 等于 3 的情况.

考察以 AC 为一对角线的平行四边形,易见

$$AB + BC = AG + HJ + KL + MN + GH + JK + LM + NC.$$

不论取 n 为多么大的数,这个等式都成立.现在令 n 无限增大.这时线段 AG,GH 等等将变得越来越短.于是点 G、J、L、…将 [79]

---

① H.E. Dudeney, The Canterbury Puzzles, London, 1919, pp. 51—54.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



无限靠近线段 AC，并且终于要落在它上边．这样一来，线段 AG 与 GH 的长度之和将等于 AH 的长．所以

$$\begin{aligned} AB + BC &= AH + HK + KM + MC \\ &= AC, \end{aligned}$$

这又是一个不可能的结论．

第四个谬论 证明任一三角形都是等腰的．

令 ABC 为任一三角形．设 D 为边 BC 的中点．过 D 作 DO 垂直于 BC．作角 BAC 的平分线交 BC 的中垂线于 O．

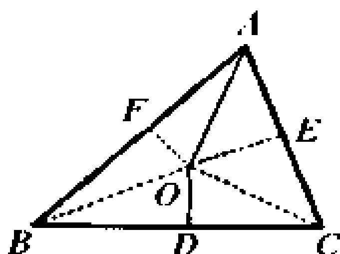


图 3.4

首先，若角 BAC 的平分线延长时不与 BC 的中垂线相交，则两者平行．于是此分角线应垂直于底边，所以 $AB = AC$．

其次，若角 BAC 的平分线延长时与 BC 的中垂线相交于点 O，作 OE 垂直于 AC，作 OF 垂直于 AB．连 OB，OC．

先考虑点 O 落在三角形内的情况，此时点 E 落在 AC 上，点 F 落在 AB 上．

三角形 AOF 与 AOE 全等，因为 AO 是公共边，角 OAF = 角 AOE，且角 OFA = 角 OEA．所以 $AF = AE$．再者，三角形 BOF 与 COE 全等，因为 OD 垂直平分 BC 而有 $OB = OC$、又因三角形 AOF 与 AOE 全等而有 $OF = OE$，还有，由作图知角 BFO 与角 CEO 皆为直角．所以三角形 BOF 与 COE 全等．于是 $FB = EC$．

所以 $AF + FB = AE + EC$，即 $AB = AC$．

以上的论证也包括了角 A 的平分线过 BC 中点的情况，以
[80] 及角 A 的平分线与 BC 的中垂线相交于三角形外部而距 BC 很



近使 E 与 F 落在 AC 与 AB 上而不是落在它们的延长线上的情况.

最后考虑 DO 与 AO 交于三角形外部而且 E 与 F 落在 AC 与 AB 的延长线上的情况.作 OE 垂直于 AC 的延长线,并作 OF 垂直于 AB 的延长线.连 OB,OC.

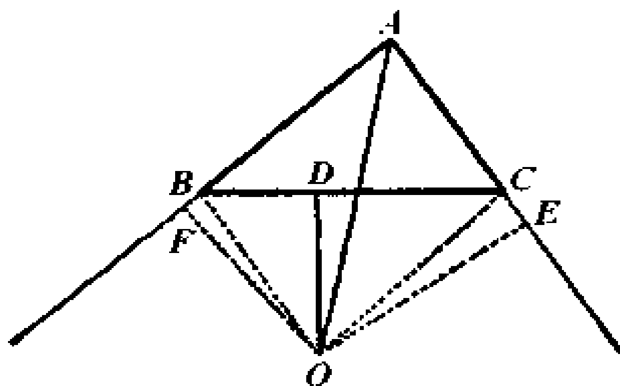


图 3.5

仿照前边的论证,由三角形 AOF 与 AOE 全等而得 $AF = AE$.又由三角形 BOF 与 COE 全等而得 $FB = EC$.所以 $AE - FB = AE - EC$,即 $AB = AC$.

于是,在各种情况下,不管 DO 与 AO 相交不相交,也不管它们交于三角形外或内,都得到 $AB = AC$.所以,任一三角形都是等腰三角形.这个结论是不可能的.

第五个谬论① 证明 $\pi/4$ 等于 $\pi/3$.

在等边三角形 ABC 内以 BC 为斜边作一等腰直角三角形 BCD.在 CA 上取一点 H 使 $CH = CD$.设 BD 的中点为 K.连 HK,延长后与 BC 的延长线交于 L.过 DL 的中点 M 作垂线与 HL 的中点 N 作垂线,设二者交于 O(在 ABC 之外,角 DKL 之 [81]
内,距 AB 颇远处).连 OC,OD,OH,OL.

---

① 这个机智的谬论是特顿(Turton)上校编制的,它首次出现于本书第三版出版时.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

由于三角形 OMD 与 OML 全等，故 $OD=OL$. 同样，由于三角形 ONL 与 ONH 全等，故 $OL=OH$. 所以 $OD=OH$. 再看三角形 OCD 与 OCH. 因为 $CD=CH$（由作图知），$OD=OH$（已证），OC 是公共边. 所以角 OCD 等于角 OCH，因而角 BCD 等于角 BCH. 前者是 $\pi/4$，后者是 $\pi/3$，故 $\pi/4=\pi/3$，这显然是荒谬的.

第六个谬论[①] 证明若一四边形的两个对边相等，则另两个对边必平行.

令 $ABCD$ 为一四边形，其边 AB 等于 DC. 过 AD 的中点 M 作垂线并过 BC 的中点 N 作垂线.

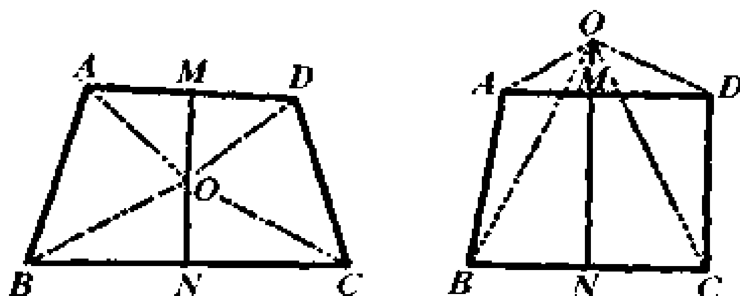


图 3.6

若此二中垂线平行，则 AD 与 BC 也平行是显然的.

若此二中垂线不平行，设它们的交点为 O，则 O 可能在四边形内（如图 3.6 左图），也可能在四边形外（如图 3.6 右图）. 连 OA，OB，OC，OD.

因 OM 是 AD 的中垂线，故 $OA=OD$. 且角 OAM 等于角 ODM. 同理，$OB=OC$，且角 OBN 等于角 OCN. 据假设，$AB=DC$，故三角形 OAB 与 ODC 的对应边皆相等，因而两个三角形全等. 所以角 AOB 等于角 DOC. 图 3.6 左图中

$$\text{左}\ \angle MON=\angle MOA+\angle AOB+\angle BON$$
$$=\left(\frac{\pi}{2}-\angle OAM\right)+\angle AOB+\left(\frac{\pi}{2}-\angle OBN\right)$$

---

① Mathesis, October 1893, Series 2, Vol. Ⅲ, p. 224.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$$=\left(\frac{\pi}{2}-\angle ODM\right)+\angle DOC+\left(\frac{\pi}{2}-\angle OCN\right)$$
$$=\angle MOD+\angle DOC+\angle CON$$
$$=\text{右}\angle MON.$$

所以角 MON 是平角，MON 为一直线，它是 AD 与 BC 的公垂线．故 AD 平行于 BC．右图中， [82]

$$\begin{aligned}\angle BOM&=\angle AOM-\angle AOB\\&=\left(\frac{\pi}{2}-OAM\right)-\angle AOB\\&=\left(\frac{\pi}{2}-ODM\right)-\angle DOC\\&=\angle DOM-\angle DOC\\&=\angle COM.\end{aligned}$$

所以 OM 是角 BOC 的平分线．但 ON 也是角 BOC 的平分线 $\left(\angle BON=\frac{\pi}{2}-\angle OBN=\frac{\pi}{2}-\angle OCN=\angle CON\right)$，故 OM 与 ON 重合而成为 AD 与 BC 的公垂线．于是 AD 与 BC 为一对平行边．

可是所得结论并非永远是对的，所以上述证明必有毛病．

第七个谬论① 下边是摘自 1889 年出版的由两位杰出的数学家编著的电学教科书的论证，它是作为正确的材料写出来的．一个给定的长度为 l 的向量可以无穷多种方式分解为两个向量 OM，MP，其长分别为 l'，l''，并且可使 l'/l'' 具有从零到无穷的任何值．假定以直角坐标系 Oxy 为参照系统，并且 OP，OM，MP 依次与 Ox 所成角为 θ，θ'，θ''．于是，把这些向量投影到 Oy 与 Ox 上而得

$$l\sin\theta=l'\sin\theta'+l''\sin\theta'',$$
$$l\cos\theta=l'\cos\theta'+l''\cos\theta''.$$

---

① 这是沙特尔先生告知我的．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$$\therefore \quad \tan\theta = \frac{n\sin\theta' + \sin\theta''}{n\cos\theta' + \cos\theta''},$$

其中 $n = l'/l''$. 不论 n 取何值，这个结果都是正确的. 既然 n 可取任何值(特别是 $n = \infty$，或 $n = 0$)，所以 $\tan\theta = \tan\theta' = \tan\theta''$. 这显然是不可能的.

第八个谬论[①] 这是关于 π 的值的一个荒谬的研究. 沿短轴切下的半个椭圆的面积(用通常的记号)等于 $\frac{1}{2}\pi ab$. 如果把中心沿长轴移到无穷远，那么椭圆退化成一个抛物线，所以在这个特定的极限情况下它的面积应该等于其外接矩形的面积的三
[83] 分之二. 不论曲线的尺寸有多大，前一个结果都是对的.

$$\therefore \quad \frac{1}{2}\pi ab = \frac{2}{3}a \times 2b.$$

$$\therefore \quad \pi = \frac{8}{3}.$$

这个结果显然是不对的.

第九个谬论 每个椭圆都是一个圆.

椭圆任一点的焦点距与横坐标的关系(依通常的记号)是[②] $r = l + ex$. 所以 $dr/dx = e$. 由此推出 r 不可能有极大值或极小值. 可是矢径既无极大值又无极小值的唯一的闭曲线是圆. 所以每个椭圆是一个圆. 这结论显然也是错的.

几 何 悖 论

我再加叙以下几个问题，它们虽非纯属谬论，但其结果乍一看时似乎是不可能的.

悖论之一 将一块平板(譬如说，一张硬纸板)旋转过四个直角使其结果与仅转过一个直角是一样的. 这是任顿(W.

---

① 这也是沙特尔先生告知我的.

② 这里 e 是离心率，l 是通径之半.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



Renton)先生告知我的一个问题.

悖论之二 像在算术中一样,概率论在几何里也提供许多悖论.这里是一个非常简单的例子.一根细棍被随机地折成三段.如果最长的一段的长度小于其余两段长度之和,也就是说,最长的一段的长度较整个细棍的长度的一半还要短,那么所折成的三段可以围成一个三角形.而一根棍折下的一段的长度小于原长之半的概率是 1/2,于是由一根细棍折成的三段能够围成一个三角形的概率似乎就应该是 1/2 了.然而这是不对的,真正的概率是 1/4.

悖论之三 下边的例子说明由实际剪割一个图形然后进行拼合各部分所得的证明是多么容易骗过眼睛的视觉.事实上,用叠合法所作的证明是很不可信的,除非有补充的数学证明.众所 [84]
周知的《几何原本》上的命题 Ⅰ.32 与 Ⅰ.47 是可以补充证明的,因而是正确的.另一方面,作为说明非数学证明是多么具有欺骗性的例子,这里叙述一个熟知的悖论:一个像棋盘那样划成 64 个小方格的正方形可以剪成四块,然后把它们拼合成一个矩形,而这个矩形却有 65 个那样的小方格①.剪与拼的方式有如下图所示.

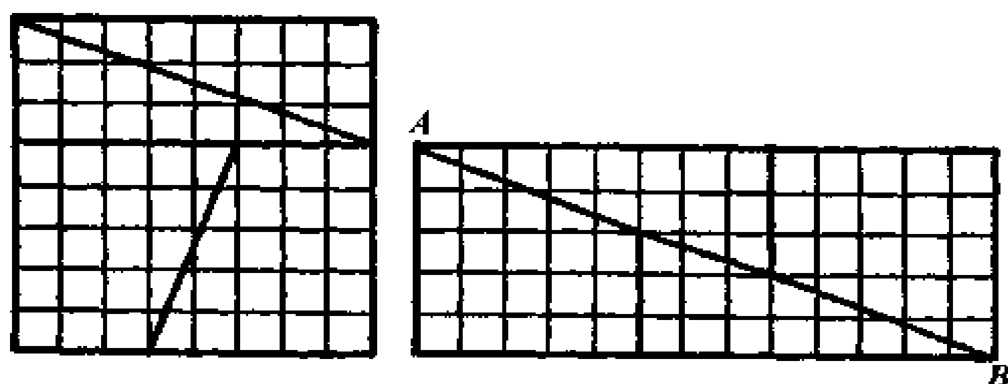


图 3.7

① 我不知道这个悖论是谁发明的.在很多书里都介绍了它.我见到的有关这个悖论的最早的文献是 Zeitschrift für Mathematik und Physik, Leipzig, 1868, Vol. Ⅻ, p. 162.奥札南在他的著作里给出了几个类似的悖论,1803 年版,Vol. 1, p. 299.

我们必须知道，而且我们必将知道



这件事之所以使一些非数学家感到费解，其原因在于第二个图中构成矩形的对角线 AB 的那些剪块的边沿并未完全叠合成对角线 AB. 事实上，它们围成一个很窄的菱形，其面积等于原正方形面积的 1/64，也就是一个小方格的面积，而其对角线 AB 较其另一对角线长得多. 从图可以看出，这个菱形的交于点 A 的两边所夹的角度是$\tan^{-1}\frac{2}{5}-\tan^{-1}\frac{3}{8}$，即$\tan^{-1}\frac{1}{46}$，这角度小于$1\frac{1}{4}^{\circ}$. 要
[85] 想用眼睛看清这么小的一个角，必须把原正方形沿图 3.7 左图中的分割线非常精细地剪开并且很细心地照图 3.7 右图拼到一起.

这个悖论的背景是等式 $5\times 13-8^2=1$. 类似的悖论可以据下列诸等式作出：

$$13\times 34-21^2=1,\quad 34\times 89-55^2=1,\cdots;$$

或者

$$5^2-3\times 8=1,\quad 13^2-8\times 21=1,\quad 34^2-21\times 55=1,\cdots.$$

这些关系都是由相邻的三个斐波那契数(见第 57 页)组成的. 一般公式

$$b_nc_{n+1}-c_nb_{n+1}=(-1)^n$$

对于任一连分式的两个相邻的渐近分数皆成立.

连分式与格点①

将一块板打上许多小方格子，在所有方格的顶点处都钉上一个小钉. 把离板的相邻两个边最近的一行和一列小钉视为坐
[86] 标轴，于是每个小钉的坐标都是非负的整数. 设 y/x 为一既约分数，则张紧在小钉(0,0)与(x,y)上的细绳将不会碰到任何别的小钉. 将细绳的一端拴死在(x,y)上，活动其另一端而不许细绳越过任何小钉. 将细绳拉紧后，把活动的一端挂在(1,0)上. 在一般情况下，它将紧靠在(1,0)与(x,y)之间的一些小钉$(x_1$,

---

① 参看 F. Klein, Elementary Mathematics, New York, 1932, p.44.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

y_1),(x_2,y_2),…上.如果活动端不是挂在(1,0)上而是挂在(0,1)上,那么它将紧靠在另一些小钉(x_1',y_1'),(x_2',y_2'),…上.可以证明 $y_1/x_1,y_2/x_2,\cdots$与 $y_1'/x_1',y_2'/x_2',\cdots$分别是 y/x 的强弱相间的渐近分式.(y_r'/x_r'出现在 y_r/x_r 之前或后,视 y/x 小于或大于 1 而定.)

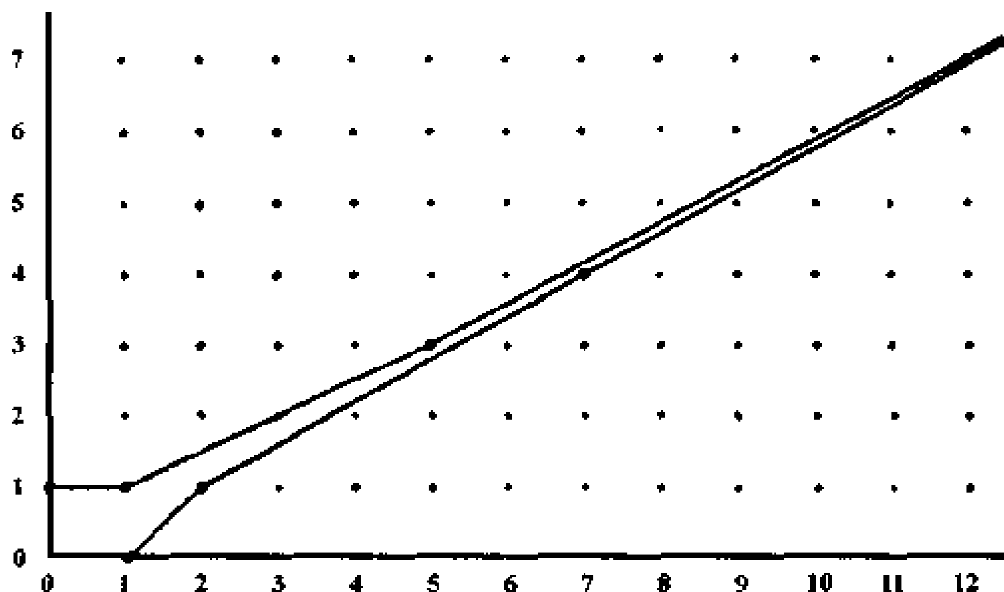


图 3.8

这个制作清楚地显示出了渐近分式接近于 y/x 的性态——强弱交错.分数 y/x 是细绳在原先张紧在(0,0)与(x,y)之间时的"斜率".这些观念不难被推广到斜率为无理数的情况,此时细绳须拴死在"无穷远处"的某个小钉上.上图表示的是斜率为

$$\frac{1}{e-1}=1/1+1/1+1/2+1/1+1/1+1/4+1/\cdots$$

的情况.注意,张紧在(1,1)与(5,3)之间的绳段接触到(但不是"压紧"在)小钉(3,2)上.分数$\frac{2}{3}$是"中介渐近"分式之一,它与通常的"主"渐近分式$\left(\frac{0}{1},\frac{1}{1},\frac{1}{2},\frac{3}{5},\frac{4}{7},\frac{7}{12},\cdots\right)$在一起构成最佳近似分数集.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

我们知道，若 b_{n-1}/c_{n-1}，b_n/c_n，b_{n+1}/c_{n+1}为任一连分式的三个相邻的(主)渐近分式，则

$$b_n/c_n=(b_{n+1}-b_{n-1})/(c_{n+1}-c_{n-1}).$$

这个等式的几何意义就是：从(0,0)到(c_n，b_n)的连线平行于从(c_{n-1}，b_{n-1})到(c_{n+1}，b_{n+1})的连线.

几 何 剖 分

一类众所周知的问题是要用直线把一个给定的平面直线多
[87] 边形剖分成几块，使它们能够拼成另一些指定的形状.它们也是一类几何游戏的内容.

毕达哥拉斯剖分 欧几里得所给的对于毕达哥拉斯定理的证明(卷 1，命题 47)是繁冗的而且不易记忆.一个优美得多的证明归功于印度数学家阿耶波多(Arya-Bhata，生于公元 466 年).为了证明任一直角三角形 ABC 的三个边长 a，b 与 c(斜边长)符合等式 $a^2+b^2=c^2$，他把这三角形的四个复制品放到边长为 $a+b$ 的正方形里，如图 3.9 中左图所示.在这个安排里剩下的部分是边长为 a 及 b 的两个正方形.在另一个安排(如图 3.9 中右图所示)剩下的是一个边长为 c 的正方形.

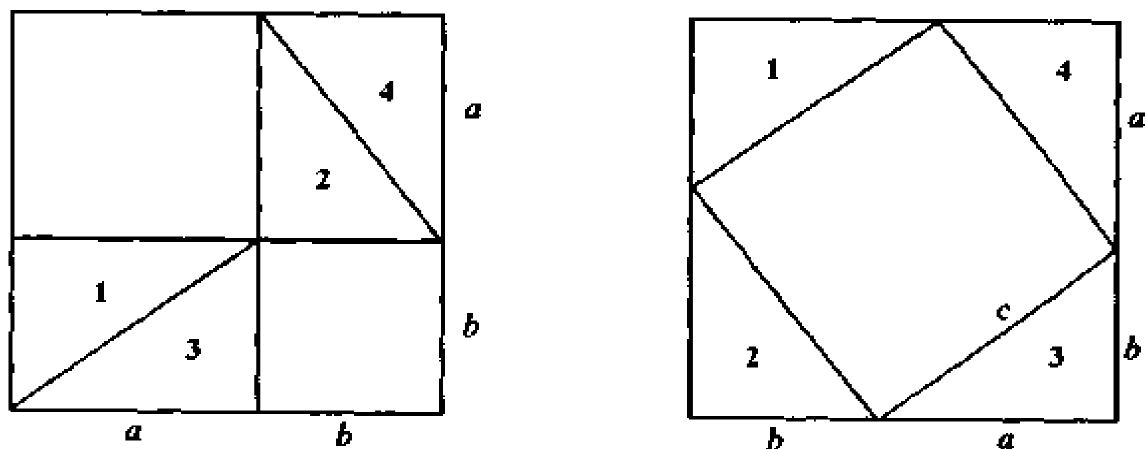


图 3.9

我们必须知道，而且我们必将知道

http://maths352.bokee.com

按希尔伯特(D.Hilbert)的《几何基础》(*Chicago*,1902,p.58)一书中的语言来说,这两个较小的正方形和一个较大的正方形被证明了“具有相等的容度(*inhaltsgleich*)”.更令人满意的恐怕是证明它们“有相等的面积”或者“有相同的分割(*zerlegungsgleich*)”.佩里伽尔①(H.Perigal)完成了这种改善,他把以 a,b 为边长的正方形 AG 与 DF 边靠边地放到一起,如图 3.10 所示(其中 $AH = HG = a$,$DE = EF = b$,且 $a \geqq b$).割线 BH 和 BE 把合并的区域分成三块,其中有两个三角形的边长都是 a,b,c.把这两个三角形 ABH 和 BDE 移到新的位置 FEC 和 HGC 上去, [88]
就产生了边长为 c 的正方形 $BECH$.

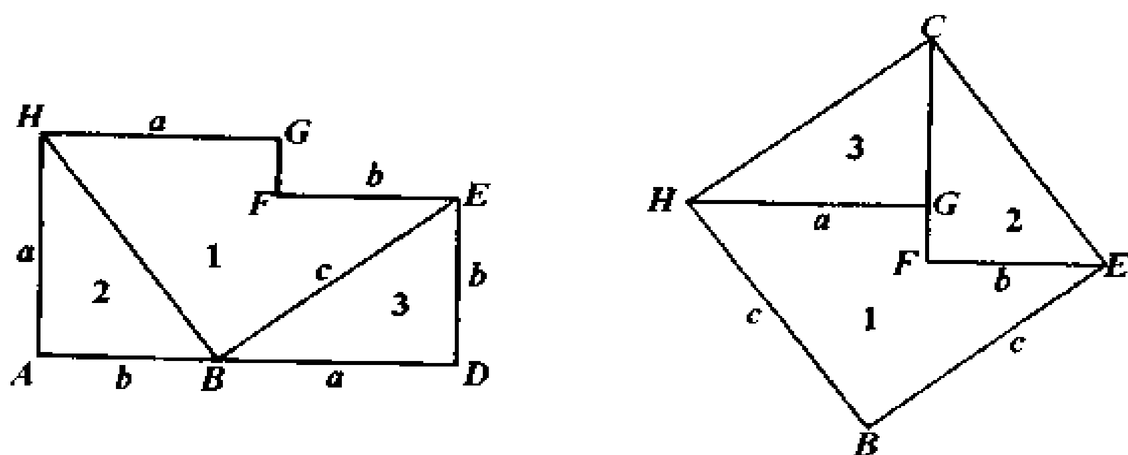


图 3.10

蒙蒂克拉(Montucla)剖分 几个类似的命题的证明流行已久,但直到 18 世纪末才由蒙蒂克拉重新引起对于这种证法的注意,他还提出并且解决了长方形的剖分问题,要求剖分后能够再拼合成一个正方形.他还解决了这个问题的反问题.稍后,巴斯乔普(P.Busschop)与德科特庞特(de Coatpont)给出了这个问题的其他解法,他们分别作出了七块剖分法与八块剖分法.前一

① H.Perigal, Messenger of Mathematics, 1873, Vol. Ⅱ, N.S., pp.103—106; H.E. Dudeney, Amusements, London, 1917, p.32.

我们必须知道,而且我们必将知道

[redacted]

位还把一个正六边形剖分成五块而拼合成一个正方形，又把一个正五边形剖分成七块而拼合成一个正方形①.

多边形的剖分 波尔约(G. Bolyai)提出了更一般的问题：要求剖分具有任意多个边的多边形，并且把剖成的各部分重新拼合成另一个具有相同面积的多边形．热尔文(P.Gerwin)已给出了一个解法．这个问题有时仍然引起人们的注意．1854年欧泽特(M.Euzet)给出了剖分多边形而拼合成三角形的方法．1895
[89] 年吉特尔(E.Guitel)讨论过更广泛的剖分两个多边形的问题，1896年霍尔斯特(E.Holst)②也讨论过这种问题，最近还有米诺(A.Mineur)③.

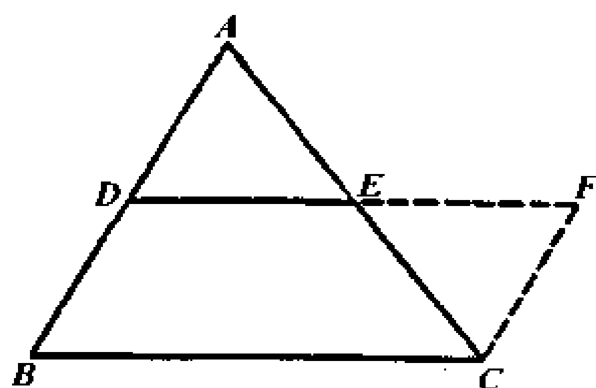


图 3.11

① Ozanam's Récréations mathématiques, 1803. 英文版, Vol. Ⅰ, pp. 292—298; 1840年版, pp. 127—129; Paul Busschop, Nouvelle Correspondance Mathématique, Brussels, 1875, Vol. Ⅱ, p. 83; de Coatpont, 同书, 1876, Vol. Ⅲ, p. 116.

② P. Gerwien, Crelle's Journal, 1833, p. 228; M. Euzet, Nouvelles Annalles de Mathematiques, 1854, Vol. Ⅷ, pp. 114—115; E. Guitel, Association Française pour l'Avancement des Sciences, 1895, pp. 264—267; E. Holst, L'Intermédiaire des Mathématiciens, 1896, Vol. Ⅲ, pp. 91—92.

③ 参看 Mathesis, 1931, pp. 150—152. 以下的论述属于戈尔德贝格(M.Goldberg).

我们必须知道，而且我们必将知道

http://maths352.bokee.com

首先考虑如何剖分一个给定的三角形而把它拼合成一个具有给定的底长的矩形.在图 3.11 中,直线段 *DE* 平行于所给三角形 *ABC* 的底边 *BC* 并平分两腰,它把三角形剖分为两部分,这两部分可以拼成一个平行四边形 *BCFD*.然后以 *B* 为中心并以给定的底长为半径画圆弧.作剖分线 *CH* 切于此弧,并作剖分线 *BG* 垂直于 *CH*.点 *G* 可能位于平行四边形之内,如图 3.12,也可能位于平行四边形之外,如图 3.13.在后一情况下,在 *CH* 上找一个点 *J* 使 *CJ* = *HG*,并作剖分线 *JL* 平行于 *BG*.于是这些碎 [90]
块可以装配成所要的矩形 *BGJK*.若底长 *BG* 太长或太短以致不能直接按上述步骤进行,那就要先改变平行四边形 *BCFD* 的边长之比.为此,把它剪成三块并重新拼合如图3.14(其中 *E′F* =

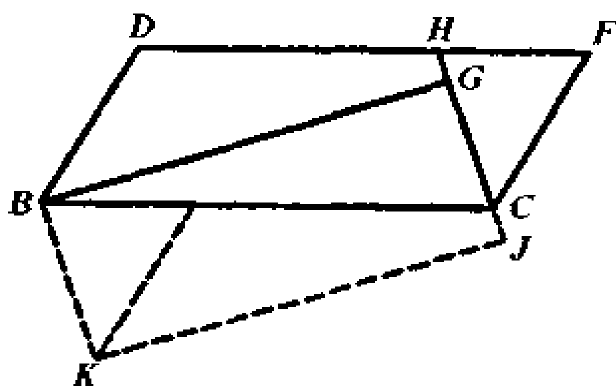


图 3.12

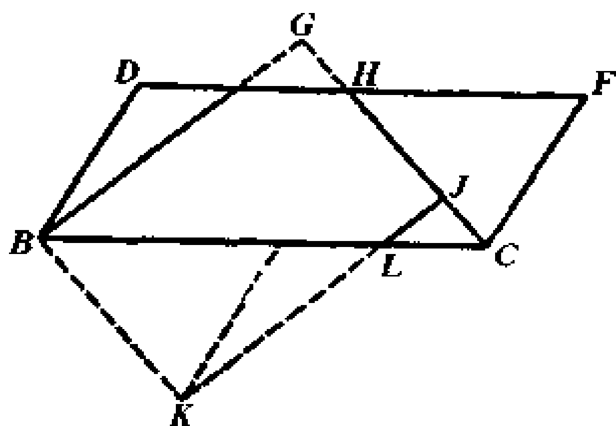


图 3.13

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

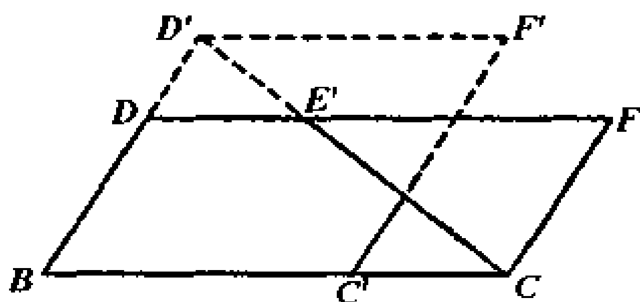


图 3.14

$BC' \geqslant \frac{1}{2}BC$). 当然,如果矩形的底长正好等于和三角形有相同面积的正方形的边长,那么三角形就被转化成一个正方形.

每个多边形都可用充分多的对角线剖分成一些三角形.所以每个多边形都可以转化成一个正方形或矩形.为此只需把剖得的每个三角形转化成具有相同底长的矩形,然后把它们叠成一列.

我们恒可以矩形为中转图形而把一个多边形转化为另一个
[91] 多边形.作成了把所给多边形以及所要多边形化为同一矩形的剖分之后,我们先用第一种剖分法把所给多边形转换成矩形,然后再用和第二种剖分法相反的步骤把矩形转换成所要的多边形.

最小剖分　前边提到的作者们的目标都是只要找到一种解法.一般地,他们都不追求最小的剖分块数.1905 年,泰勒(H.M. Taylor)①给出一些特殊情况的解,其中包括两个三角形互化的四块剖分、一个三角形和一个平行四边形互化的四块剖分、两个平行四边形互化的四块剖分,他认识到求最小剖分块数的需要.

巧剖　杜德尼最近提出了此类种种巧妙的难题,在所有情况下,剖分的块数都是预先指定的②.他的声望使得此类问题引

① Messenger of Mathematics, Vol. XXXV, pp. 81—101.

② 例如,参看他的 Amusements in Mathematics, London, 1917, p.27 起以后.

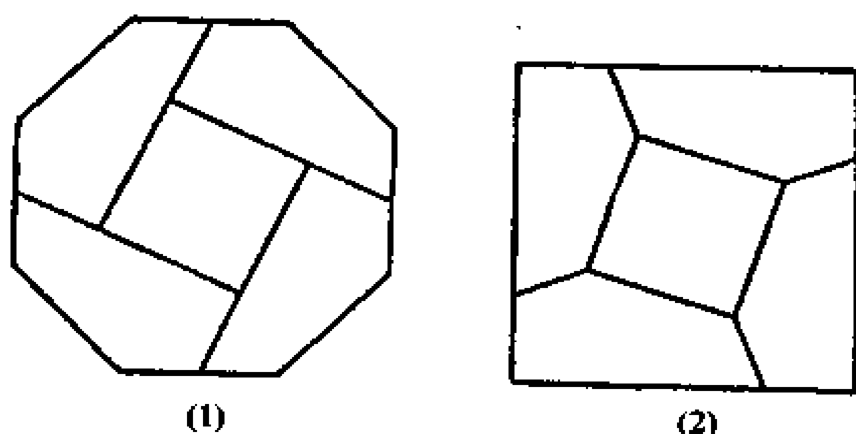
我们必须知道，而且我们必将知道

http://maths352.bokee.com

人注意.作为此类几何游戏的例子,我摘录他的几个问题来:(a)用两条直线剖分一个希腊十字(即由五个相同的正方形组成的十字)成为形状和大小都一样的四个部分,并要这四部分能够拼合成为一个正方形;(b)将一个等腰直角三角形剖分成四块,
使它们能拼合成一个希腊十字;(c)将一个正五边形剖分成六 [92]
块,使它们能拼合成一个正方形;(d)将一个等边三角形剖分成四块,要它们能够拼合成一个正方形.

对于这类问题感兴趣的读者会愿意去比较一下最后这个问题的杜德尼解和上边说到的泰勒所给的解,以及下边引证的麦考利(W.H.Macauly)所给的解.

惠勒(A.H.Wheeler)与戈尔德贝格①曾把一个正五边形剖分成六块,并将它们拼合成一个等边三角形;特拉弗斯(J. Travers)曾把一个正八边形剖分成五块,并将它们拼合成一个正方形(见图3.15).



(1) (2)

图 3.15

麦考利的四块剖分 麦考利②讨论了两个面积相等的直边

① American Mathematical Monthly, 1952, Vol. LIX, pp. 106—107.

② Mathematical Gazette, 1914, Vol. Ⅶ, p.381; Vol. Ⅷ, 1915, pp. 72, 109; Messenger of Mathematics, Vol. XLVIII, 1919, p.159; Vol. XLIX, 1919, p.111.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



形的四块剖分的理论.他论述了两个三角形的、一个三角形和一个平行四边形的、两个四边形的、两个具两个相等且平行的边的五边形的以及两个有一定关系的六边形的四块剖分问题.他的结果是射影的并且所有他的结果都可以从他的六边形的剖分推导出来.这是一个有趣的推广.

立体剖分　自然要问,是否每个多面体也可以用有限张平面去剖分它,使剖得的子块能够嵌合成任意其他具有相同体积的多面体?答案是否定的.德恩(M.Dehn)①证明了:不是每一个四面体都能够经过剖分而转化成一个棱柱体.这就杜绝了对于立体的剖分像多边形的剖分那样找到一个一般方法的希望.不过,一些特殊立体的剖分是完全可能的.

二倍立方体　下面是"德利安(Delian)问题"(我们将在第12章里论述它):给你一条长度为 $2^{1/3}$(即$\sqrt[3]{2}$)的线段.请用平面
[93] 把棱长为1的两个正方体剖分成子块,并将它们嵌合成一个正方体.这个问题可以经两次运用把一个给定的矩形转化为一个具有给定底边长的矩形而解决."最小"剖分可用图3.14而不是用图3.12的方法而得到.

先把这两个相等的正方体靠到一起而构成一个 $2\times1\times1$ 的正方柱体.然后在它的一个矩形侧面(2×1)上画上为了把这个矩形转化为一个底边长为 $2^{1/3}$ 的矩形而需要的切口,这个长度即是体积为2的立方体的棱长.用通过这些切口并垂直于该侧面的两个平面依次把长方柱体剖成三块.

将这三块装配成一个新的长方柱体 $2^{1/3}\times2^{2/3}\times1$.最后,随便在哪一个尺寸为 $2^{2/3}\times1$ 的侧面上画上为了把这个矩形转化为一个底边长为 $2^{1/3}$ 的矩形而需要的切口.再用通过这些切口并且垂直于该侧面的两个平面依次把新的长方体再剖

---

① 参见 H.C.Lenhard, Elemente der Mathematik, 1962, Vol.XVII, pp.108—109.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

成三块，就可以把它们装配成所要求的立方体了．原先的 $2\times1\times1$ 的棱柱体被剖分成七块不规则的立体．如果把这些子块弄乱，要把它们再装配成一个立方体或者棱柱体也不是一件容易的事．

这个问题是小切尼(W.F. Cheney Jr.)提出的．它的上述解法是 A·H·惠勒①给出的．

割 圆 术

高斯②在 17 岁时证明了：若 p 为素数，则每当 p 为数 F_m（依第 69 页的记号）之一时，求解“割圆方程”$x^p=1$ 的问题总可归结为一系列求解二次方程的问题．稍后③，旺策尔(P. L. Wantzel)把这个“每当”强化为“当且仅当”．由于割圆方程的根是

$$\cos(2r\pi/p)+i\sin(2r\pi/p)\quad(r=0,1,\cdots,p-1),$$

所以当且仅当 n 为一“费马素数”F_m 或几个不同的费马素数的乘积时，一个奇数个边的正 n 边形可以用欧几里得作图（即用直尺和圆规作图）法作出来．因为一个 $2^k n$ 边形的作图包括着一 [94]
个正 n 边形的作图，跟着 k 个二等分角，所以只须考虑奇的 n 值．

如果我们假定 F_4 以后的费马数都是合数，那么④n 必须是 3，5，17，257，65 537 或 $2^{32}-1=4\ 294\ 967\ 295$ 的一个因子．如果一个可用直尺和圆规作出的正多边形的边数为更大的奇数，那么这个大的奇数必至少有 39 457 位，因为第一个尚未弄清楚是

① American Mathematical Monthly, 1935, Vol. XLII, p.509.

② Disquisitiones Arithmeticae, 1801.

③ Liouville's Journal de Mathematiques, 1837, Vol. II, pp. 366—372.

④ Kraïtchik, La Mathematique des Jeux, Brussel, 1930, p.99.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

否合数的费马数是 $F_{17}(=2^{131072}+1)$.

正三角形和正五边形的作图法是人所熟知的.由此,马上可以作正 15 边形,因为 $\frac{4\pi}{5}-\frac{2\pi}{3}=\frac{2\pi}{15}$;你只须在一个圆内作出一个内接正三角形和一个内接正五边形.下述正 17 边形的作图法是里奇蒙德(H.W. Richmond)给出的,他还给出了一个正五边形的作图法以资对比.

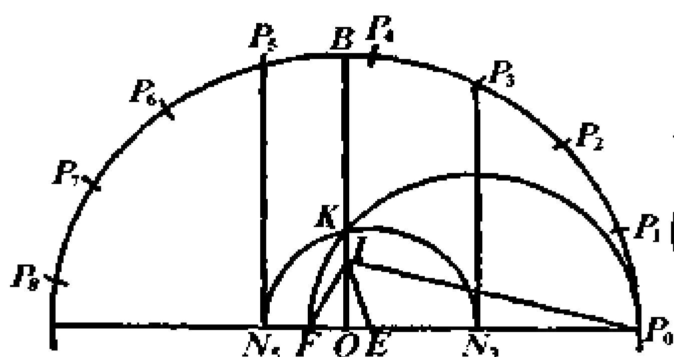


图 3.16

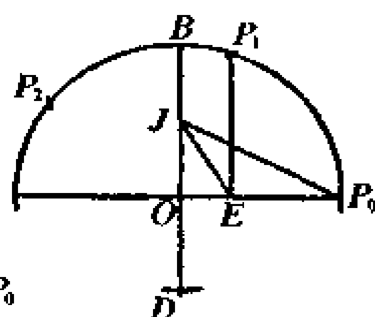


图 3.17

问题是要在一个给定的圆内作一内接正 17 边形,以 P_0 为顶点之一(参看图 3.16).令 OB 为垂直于过 P_0 的直径的一个半径.在 OB 上取一点 I,使 $OI=\frac{1}{4}OB$.连 IP_0,并在 OP_0 上取点 E、F,使 $\angle OIE=\frac{1}{4}\angle OIP_0$ 且 $\angle FIE=\frac{1}{4}\pi$.设以 FP_0 为直径的圆交 OB 于 K,并设以 E 为中心、以 EK 为半径的圆交 OP_0 于 N_3(在 O 与 P_0 之间)及 N_5(在 O 与 P_0 之外).作平行于 OB 的直线 N_3P_3,N_5P_5,分别和原来的圆交于 P_3,P_5.于是弧段 P_0P_3
[95] 与 P_0P_5 将分别是圆周的 $\frac{3}{17}$ 与 $\frac{5}{17}$.

证明①包含着重复应用这样一个事实:方程 $x^2+2x\cot 2C=1$ 的根是 $\tan C$ 与 $-\cot C$.

① Quaterly of Journal of Mathematics, 1893, Vol. XXVI, p.206.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

对于正五边形①(图 3.17)的问题,像前边一样确定 B.设 OB 的中点为 J.在 OP_0 找一点 E,使 JE 平分角 OJP_0.过 E 作平行于 OB 的直线交圆于 P_1,则弧 P_0P_1 就是圆周的 $\frac{1}{5}$.

马上可以作 51 边,85 边与 255 边的正多边形;还可以作边数为这些数与 2 的任何次幂的乘积的正多边形.

仅用圆规作图

大家知道欧几里得在他的《几何原本》中所论的作图题都是限于仅用无刻度的直尺和圆规能解决的问题.然而直尺的使用也并非必要的②.马歇罗尼(Mascheroni)③藉仅用圆规所完成的作图证明了一连串的命题.当然,其间的逻辑顺序与我们熟悉的逻辑顺序大不一样.

作为说明这个情况的例子,我选取求两已知点 A 与 B 的中点的问题.对于这个基本命题,马歇罗尼给出了五种解法(命题 66).下边是它们之中的两个.它们的根据都是这样一个命题:已知圆心和圆上一点,可以作一个半圆.这个命题是他先已证明过的.每种证明都是很简明的.这个命题已有别的解法,其中有些连半圆也不用作了.

他的作图法之一如下:以 B 为中心、BA 为半径作半圆,A [96]
和 C 是半圆的直径两端.再以 A 与 C 为圆心、分别以 AB 与 CA

---

① 杜德尼提出了正五边形的一个较简便的作法,参看他的 Amusements in Mathematics, p.38. 以 J 为中心、JP_0 为半径画圆弧交 BO 的延长线于 D.于是以 P_0 为中心、P_0D 为半径的圆弧将交原来的圆于 P_1.

② Michael Goldberg, School Science and Mathematics, 1925, Vol. XXV, pp. 961—965.

③ 他的著作于 1797 年在 Pavia 出版.不过,最近才知道他的大部分结果早已由莫尔(G. Mohr)发表过.莫氏的 Euclides Danicus 于 1672 年在 Amsterdam 出版(1928 年又在 Copenhagen 出版).

我们必须知道，而且我们必将知道

为半径作圆.设它们的交点为 P 与 Q.再以 P 与 Q 为圆心并以 AB 为半径作圆.它们将相交于 AB 的中点.

为了某些目的,他宁愿用另一个解法.这个解法是:以 B 为中心、BA 为半径作半圆,A 与 C 是这半圆直径的两端.再以 A 与 C 为圆心、AB 为半径作圆.它们分别和半圆相交于 H 和 K.再以 A 与 C 为圆心、AC 为半径作圆,它们分别与上述两圆相交于 Q 和 P.最后再以 P 与 C 为圆心、分别以 PA,PQ 为半径作圆.这两个圆的交点之一就是 AB 的中点.

任何人都可以编造许多此类几何游戏,因为需要的只是随便选取欧几里得的一个命题,然后看怎样只用圆规去解决它.例如,我选:求作一三角形,要它的底边在一条给定的直线上并且和一个给定的三角形相似;或者:求作一正五边形,它的大小是给定的.不管你是怎样解决的,看一看马歇罗尼的书上是怎么个解法,总是有趣的.

五 圆 覆 盖

用五个较小的同样大的圆白铁片一个个放到一个固定的红色圆盘上,要求将这圆盘完全盖住.常逛英国集市的人对此问题是熟悉的.问题之所以困难,在于设局人已把白铁片做到了尽可能地小.这就引出一个有趣的几何问题:求能满足问题要求的圆白铁片的最小半径.

如果圆白铁片的半径比红色圆盘半径的五分之三稍大一些,则问题是可解的.当然,在一场游戏中,圆白铁片一放下之后就不许再移动它了.游戏者凭观察就能把圆白铁片都放到正确
[97] 位置上的事例是极少极少的.

行之有效的规则如下.设红色圆盘的中心为 O,半径为 a,而 AOB 是它的一条直径.在 OA 上取一点 P 使 OP 大致等于 $a/35$.然后把第一个圆白铁片放到这样的位置上:要它的中心在 OB 上而且 P 处于它的边沿上.假定它的边沿与红圆盘的边沿

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的交点是 C 与 C'，它们位于 AB 的不同的两侧.再把第二、第三个圆白铁片放下去，皆以 AP 为一条弦.设这两个圆片的边沿与红圆盘的边沿的交点除了点 A 之外是 D 与 D'，D 是与 C 在 AB 同一侧的点.最后把剩下的两个圆片放下去，要它们分别以 CD 与 $C'D'$ 为一条弦.于是，问题已经解决了.人们乍一想时，会以为把圆白铁片的中心放在红色圆盘的内接正五边形的顶点上时，所需圆白铁片的半径最小，其实不是的.

实际上为了简便，最好是把圆白铁片做得比理论上的最小值稍大一些，并且将 P 视为与 O 重合的点.

这个问题的数学论证过于冗长，不宜在此介绍.恐怕大多数读者所想要知道的只是上述结果的简略介绍.如果要更精确的近似值，下边就是①.若把红圆的半径取为一尺，则小圆片的临界半径为 0.609383 尺，再短则问题就成为不可能的了.相应地 $OP = 0.028547$ 尺.所以 O 离第一个放下的小圆片很近，但并不在它的边沿上.如果让三个小圆片的边沿都碰到 O，那么它们每一个的半径都必须长于 0.6099579 尺.实际上这个长度与最小圆片半径是难以辨别的.如果把所有的小圆片的中心都放在内接正五边形的顶点上，并且要它们的边沿都通过点 O，那么它们每一个的半径都必须大于 0.6180340 尺.所以，除非小圆片做得非常精确，可以让每一个小圆片的边沿都通过点 O 而解决问题.作为一个难倒人的游戏，又有这个粗略法则的可用，这是本问题的一个严重的弱点. [98]

我相信集市上所用的小圆片一般地都大得足可运用上述粗略法则，尽管如此，仍以运用正确法则为比较安全.在我给自己做的一个实例中，我在红圆中心的附近做了一个颜色很淡而微小的记号，但是离中心又足够远，使想让每个小圆片的边沿都通

① 参看 E.H. Neville, proceedings of the London Mathmatical Society, 1915, second series, Vol. XIV, pp. 308—326.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

过该点的人都必定失败.虽然游戏主持人忽视了正确的法则或者对之无知,他们似乎觉得这种游戏是有利可图的.显然,从他们的观点看,这是它的价值的极好检验.

勒贝格极小问题

这是关于覆盖一个区域的尚未解决的问题.任一图形的直径指该图形中任意两点间连线之最长者.勒贝格(Lebesgue)的问题①是求*面积最小的平片,当适当放置它时,它能够遮盖住任何一个直径为1的平面图形*.

单位圆片太小了,因为它虽然能够遮盖住具有单位对角线的正方形,却遮盖不住边长为1的正三角形.另一方面,外切于单位圆的正六边形又大得没有必要.因此,所求的平片的面积当介于$\frac{1}{4}\pi$和$\frac{1}{2}\sqrt{3}$之间.它的精确的大小和形状还从未找到.

挂谷宗一极小问题

和勒贝格的极小问题有点类似的一个问题是:求一单位长的有向线段在平面上作连续运动直到它回到原来的位置(但方向颠倒过来)时所扫过的最小面积.挂谷宗一(S.Kakeya)的问题曾经算得上是一个著名的未解决的问题,不过,在它被提出仅仅十年之后,它的彻底解决已被公布出来了.奥斯古德(Osgood)与洼田忠彦(Kubota)猜想三尖形(即三尖圆内旋轮线所围成的区
[99] 域)是一个可能的解,它的面积恰为直径为1的圆的面积的一半(参看图3.18).

---

① Julius Pál, K.Danske videnskabernes selskab, Copenhagen. Mathematisk-fysiske meddelelser, 1920, Vol.Ⅲ, no.2, pp. 1—35; S. Kakeya, Tôhoku Sience Reports, 1917, Vol. Ⅵ, pp. 71—78; Coxeter, Eureka, 1958, Vol. XXI, p.13.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

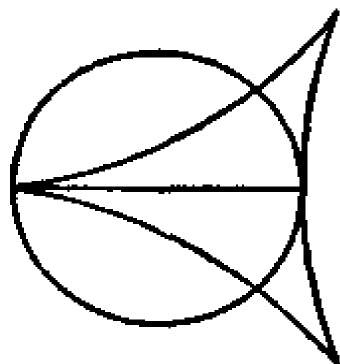


图 3.18

别济科维奇(Besicovitch)曾证明①没有最小的面积，面积可以任意地小！这个惊人的结果是难以置信的，所以我要给出他的优美的证明的要点.

只需说明一个图形它能容许单位长的线段在它里边转过一个直角就够了，因为只要把两个那样的图形拼起来就构成一个具有挂谷宗一性质的图形. 从一个三角形 ABC 入手，其中 $AC = BC$，C 是直角，由 C 到 AB 的高等于 1. 开始时位于 AC 上的单位线段显然可以在三角形内转至 BC 上. 别济科维奇的想法是逐渐完成这个旋转. 在 AB 上取很多均匀分布的点，用 C 和它们的连线把三角形 ABC 剖分成很多窄的三角形. 然后把它们分别沿 AB 移过一个不同的距离，同时保持其大小、形状、定向都不变，使它们尽可能地重叠起来. 别济科维奇一方面把三角形剖分的个数取得充分大，一方面把每个窄三角形进行一个适当的移动，使最终所得图形的面积达到任意地小. 不过，虽然一个线段能够在这个图形内进行许多微小的转动，但却不能连续地转过整个直角，因为还不能够从一个窄三角形进入下一个窄三角形. 这个缺点可以用所谓“铰结”——即连结相继的窄三角形的 [100]
通路去扩大图形而纠正它. 为了减小这些铰结的面积，须把它们

① A.S. Besicovitch, Mathematische Zeitschrift, 1928, Vol. XXVII, p.312.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

做得颇为纡回.每个铰结由两条很长的几乎平行的直线段构成,每条由要连结的窄三角形之一发出,两者相交于另一个很窄的高度取为1的三角形.每个铰结的两条直线之间的狭长地带的面积不计入图形的面积.这就使最终所作的图形是一个带花边的蛛网状的东西,从它辐射出许多狭窄的回线达到很远的地方.

一些年来,数学家们一直在揣摩别济科维奇图形的贯穿性与远伸性是否可以避免.剩下的学术问题是:具有挂谷宗一性质的单连通(且(或)有界)集的面积可能小到什么地步?(没有孔洞的集合称为单连通的.)顺便说到,在一般问题的别济科维奇解之前,帕尔(J.Pál)①已经解决了关于凸集的相应问题,答案是面积为 $1/\sqrt{3}$ 的等边三角形.直到1965年才由布卢姆(Bloom)与舍恩伯格(Schoenberg)②独立地发现小于挂谷宗一自己的三尖形的具有挂谷宗一性质的单连通集;他们的例子的面积都接近于 $(5-2\sqrt{2})\pi/24$,这个数大约等于 $\pi/11$.坎宁安(F.Cunningham)发现,实际上在图形为单连通的且含于单位圆内这些限制下,答案与别济科维奇的解并无差别,仍旧能使图形的面积任意地小.

尽管如此,仍然有一个问题悬而未决.如果一个集内有一个点,它和该集的任何其他点的连线都属于该集,那么这个集就称为星形的.具有挂谷宗一性质的星形集的面积能小到什么地步?
[101] 布卢姆与舍恩贝格的例子都是星形的,它们表明,此类集中有的集可以具有和上述数值(约为 $\pi/11$)任意接近的面积.(舍恩伯格把他的那些图形的典型之一很别致地描绘了出来,它的形状很像摆动万次的傅科(Foucault)摆的摆尖的轨迹.)另一方面,坎

---

① Julius Pál, Mathematische Annalen, 1921, Vol. LXXXIII, pp. 311—319.

② F. Cunningham, Jr. and I. J. Schoenberg, Canadian Journal of Mathematics, 1965, Vol. XLII, pp. 946—956.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

宁安的例子却不是星形的.他还证明了,具有挂谷宗一性质的星形集的面积不可能小于 $\pi/108$. 于是,星形挂谷宗一集面积的下界的值(在 $\pi/108$ 和 $\pi/11$ 之间)尚待寻求.

补　　记

对 86 页的补注.可以这样完成所需的平板的旋转:假定要旋转的结果等价于绕点 O 转过一个直角.在平板上画一个正方形 $OABC$.将平板相继地以对角线 OB 为轴转过两个直角,然后再以 OA 边为轴转过两个直角.所求的结果就达到了. [102]

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第4章 几何游戏

现在撇开正式的几何命题的事项,我来列举几个游戏或动脑筋的问题,它们主要是涉及事物的相对位置.不过此类娱乐的详细讨论则有待于第10章去进行,因为需要一些算术或代数的工具.有些作者把西洋象棋、单人象棋、国际象棋之类的游戏作为几何课题,就像把骨牌戏、双陆棋与掷骰子游戏作为算术课题一样.但是这些课题的讨论所需设置的假定太多了,难以体现真实的游戏,也不大有趣.

我所挑选的游戏的说明都很简单.数学家可能会想略去这一章.有些例子很难说应该把它们划归入算术游戏或者几何游戏,不过这也无关紧要.

静态的布局游戏

在众多的涉及几何学的静态游戏之中,我只叙述三四个.

三子成行 首先,我要说说三子成行的游戏,像打叉画圈、麦瑞伊(merrillees)以及在围棋盘上玩的“五子棋”都是熟知的例子.此类游戏都是在一个棋盘上玩的,一般地,它的形状是包含n^2个小方格的正方形.通常的玩法是甲方在他所占的小方格里下上一个白色的棋子或者打上一个叉,乙方在乙所占的小方格里下上一个黑色的棋子或者画上一个圈.接下去轮流下子.谁先
[103] 占满在一条直线上且相邻的三个(或任何约定的个数)小方格,谁就算胜.如果棋盘上总共只有9个或16个小方格,要给出完

我们必须知道，而且我们必将知道

http://maths352.bokee.com

全的分析并无困难，不过是冗长的而且也不怎么有趣．此类游戏多数已为古人所知①，因此我在这里提一下．

三子成行的推广　我可以再添一个优美但比较难的推广．就我所知，前此尚未载入任何数学游戏的书中．问题是要把 n 个棋子下到棋盘上，使它们形成的行数最多，每行恰有 3 个棋子②．

容易的是把棋子安排成 N 行，N 为 $(n-1)^2/8$ 的整数部，其法如下：在三次抛物线上任取一点 P③．设点 P 处的切线交曲线于点 Q，点 Q 处的切线交曲线于点 A．令 AP 的延长线与曲线的交点为 B，BQ 的延长线与曲线的交点为 C，CP 的延长线与曲线的交点为 D，DQ 的延长线与曲线的交点为 E，等等．于是棋子应下在点 $P,Q,A,B,\cdots$ 上④．9 个棋子构成 8 行⑤；10 个棋子构成 10 行；15 个棋子构成 24 行；81 个棋子构成 800 行；等等．

西尔维斯特曾发现，如果起始点 P 选得适当，行数可以增至 $(n-1)(n-2)/6$ 的整数部分．如此，9 个棋子可以排成 9 行；10 个棋子可以排成 12 行；15 个棋子可以排成 30 行；81 个棋子可以排成 1 053 行；等等．

然而这些仍然不是最高限，行数还可以增多．例如，西尔维斯特说过 9 个棋子可以摆成 10 行，每行有 3 个棋子．我不知道

---

①　Becq de Fouquières, Les Jeux des Anciens，第 2 版，Paris，1873，第 XVIII 章．

②　Educational Times Reprint，1868，Vol．VIII，p．106；同刊 Vol．XLV，pp．127—128．

③　三次抛物线取为 $y=x^3$，点 P 须是纵横坐标皆为整数的点，如 (1,1)，但不得取原点．——译者注

④　这些点的坐标必皆为整数，它们都是棋盘上的格点．——译者注

⑤　这八行是 APB，BQC，CPD，DQE，EPF，FQG 以及 CAF，DBG．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



他是怎样摆的，不过，有一个摆法是把 1 点和 8 点分别摆在两个矩形（或者平行四边形）2365 和 4367 的中心上（这两个四边形
[104] 有一个公共边 36）. 于是连线 18，27，36，45 都交于同一个点，在该处摆上 9 点. 这时，10 个三子成行的棋子集就是那些点数为 a, b, c 而满足 $a+b+c \equiv 0 \pmod 9$ 的三元集合.

西尔维斯特提出了一个问题——是否能安排 n 个棋子（不在同一直线上），使它们之中任何两个都和另外一个共线？答案是否定的，不过，他去世之后才有人作出证明①.

p 子成行　上述问题立即可作如下的推广：把 n 个棋子下到尽可能多的行上，要每行恰有 p 个棋子. 先把一些行线的交点取在无穷远，此类问题可马上解决. 然后（需要的话）把所得图形作投影，使无穷远点变成有穷远点. 上边已给出了这种解的一个例子.

作为例子，我还可以给出 10 个棋子下成 5 行的下法，每行有 4 个子；16 个棋子下成 15 行的下法，每行有 4 个子；18 个棋子下成 9 行的下法，每行有 5 个子；以及 19 个棋子下成 10 行的下法，每行有 5 个子. 我把这些问题留给聪明的读者（参看第 132 页）.

拼砌　另一静态游戏是拼砌（或铺砌）. 它的要求是用具有给定几何形状的瓷片铺满一个平面区域. 这是一种精工镶嵌的几何设计.

如果瓷片的形状是正多边形，并且两个相邻的瓷片公有一条整个的边（或仅有一个公共顶点），则构成的图形是容易枚举的. 例如，如果限于使用同样的瓷片，每片都是正 p 边形，那么就只能用正三角形、正方形，或正六边形. 理由是，假定需要 q 个正多边形围着一个顶点砌满它的一个邻域. 由于正 p 边形的每个内角等于 $(p-2)\pi/p$，故 $q(p-2)\pi/p = 2\pi$，即

$$(p-2)(q-2)=4.$$

[105] 因为 p 和 q 都是大于 2 的，所以只须考虑把 4 分解为两个正整

---

① 参见 Coxeter, Introduction to Geometry, p.65.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

数因子的一切可能的方式.用 p^q 记此类正则拼砌(每一顶点周围有 q 个正 p 边形),则不难得知,可能的拼砌①仅有 $6^3, 4^4, 3^6$ 这三种方式.

然而,如果允许采用不同的正多边形瓷片(正三角形、正方形,等等),那么我们可以作出覆盖一个平面区域的许多种几何方案.如果围绕每个顶点的多边形的个数和形状都是相同的,并且环绕的顺序也相同(或相反),和上边相仿地分析②,得知有八种可能的砌法,即:

$$3\cdot 12^2,\quad 4\cdot 6\cdot 12,\quad 4\cdot 8^2,\quad (3\cdot 6)^2,\quad 3\cdot 4\cdot 6\cdot 4,$$
$$3^3\cdot 4^2,\quad 3^2\cdot 4\cdot 3\cdot 4,\quad 3^4\cdot 6.$$

砌法 $3^4\cdot 6$(在每个顶点处有四个三角形和一个六边形)有个特点,那就是存在着两种相反的形态,即,不能与自己的镜象叠合(除非你把整个平面反转过去).

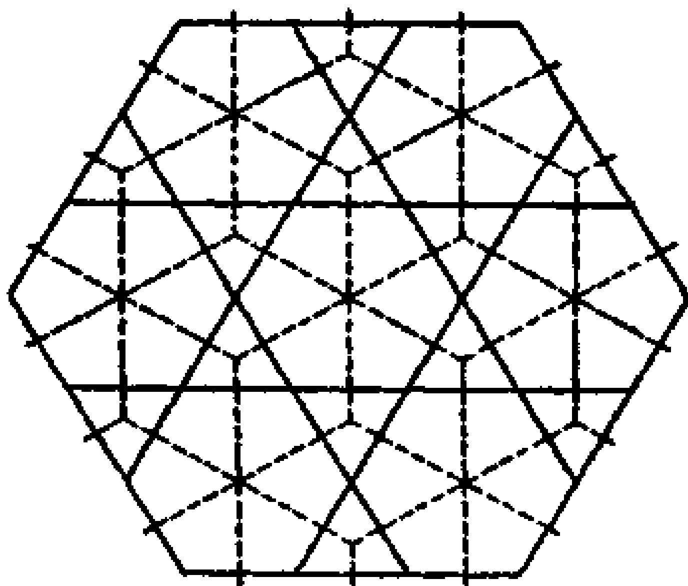


图 4.1

① 用多边形覆盖球面的类似问题和构造正多面体是等价的(参看 135 页).关于 6^3 在选举制——比例代议制上的一个应用,参看 G. Pólya, L'Enseignement mathématique, 1918, Vol. XX, p.367.

② 见 Kraïtchik, pp.272—282,图 421—423,425,426,432,433,440.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

当你把一个这样的拼砌的每条缝换之以垂直于该缝并连结 [106] 两相邻瓷片的中心的线段时，得到的是一个反拼砌，它的瓷片都是一个样子（但不一定是等边的）. 在这种意义上，6^3 是 3^6 的反拼砌（反之亦然），而 4^4 是自反的（或者说，与一个全等的 4^4 互反）. 图 4.1 中画的是拼砌 $(3\cdot 6)^2$ 和它的反拼砌.

半条反拼砌 颜色的使用引起了新的问题. 普通的棋盘① 就是由两种颜色的方格构成拼砌的一个例子，它的方格染成黑白交替的两种颜色. 西尔维斯特发明了另一种双色方块拼砌②，他称之为半条反拼砌. 如果把普通棋盘的任意两行或两列格对格地并排到一起，那么，分属两行而有相邻边的方格的颜色要么全相同、要么全不同. 在半条反拼砌（双色）里，任意两行或两列并置时，属于两行（列）的相邻方格对子中有一半是同色的、另一半是异色的.

若 m 为奇数或奇偶数，则含有 m^2 个方格的半条反拼砌是不可能的. 有人猜想只要 m 是 4 的倍数，半条反拼砌就是可能的. 第一个值得怀疑的情况是 $m = 188$.

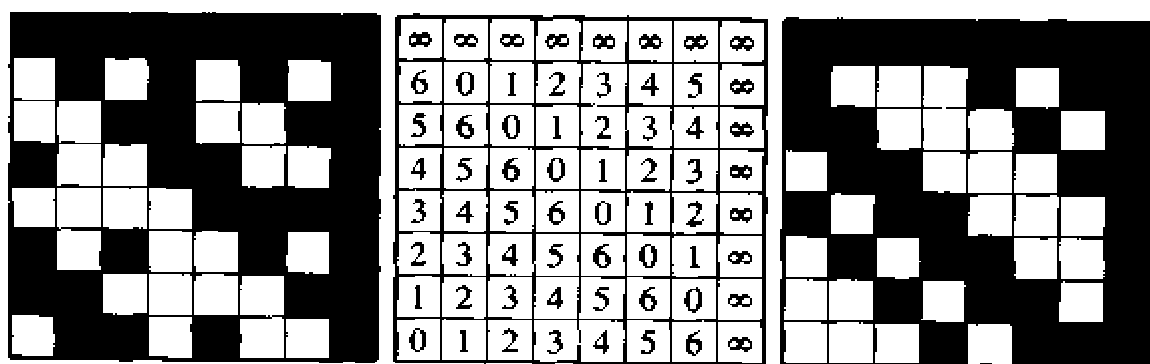


图 4.2

① 指国际象棋盘. ——译者注

② 见 Mathematical Questions from the eduational Times. London, Vol. X, 1868, pp. 74—76; Vol. LVI, 1892, pp. 97—99. 这些结论与方程论中的定理有密切的联系.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



如果知道了当 $m=a$ 和 $m=b$ 时的解，那么立即可以推出当 $m=ab$ 时的解．为此只须用整个 b 拼砌代换 a 拼砌的每一个黑格子，并用与 b 拼砌颜色相反的拼砌代换 a 拼砌的每一个白格子．重复应用这个原则可以得出 m 为 2 的任一次幂时的解．图 4.2 中第一个画的是 $m=8$ 的情况．

当 p 是形状为 $4k-1$ 的素数而 n 为奇数时，可以由GF(p^n)(参看第 75 页)的加法表推出 $m=p^n+1$ 的一个半条反拼砌如下．在表的最下一行和最左一列，我们先写下此有限域的 $m-1$ [107]
个元素和一个第 m 号“元素”∞，它的定义是当任一元素(包括它自身)和它相加的结果仍是它自身．表中其余的格子中填上其对应的最左列和最下行中元素的和(图 4.2 表明了当 $p=7$，$n=1$，即 $m=8$ 时的情况)．按照格子中的数是否一个平方而把格子染成白或黑色的并约定①∞为非平方．(依此规则，当 $m=8$ 时，数码 0，1，2，4 所占方格应为白色的，而 3，5，6，∞所占方格应为黑色的．)

图 4.3 画的是 $m=28$(相应于 $p=n=3$)的情况．按“自然”顺序排列时，数码是 0，1，2，10，11，12，20，…，221，222，∞，其中平方数是 0，1，20，21，22，100，102，110，111，120，121，202，211，221．容易验证(除了 0 以外，它们正是 10 的各次幂(即 1，10，100，12，120，…，201)序列中的第一、三、五、七、……项②．

此类问题的理论基础是达文波特与佩利(R．E．A．C．Paley)

---

① 人们会自然地以为∞是它自己的平方，就像 0 的平方是 0 一样．我避开不用“二次剩余”一词，因为 0 是平方数是无可争辩的，然而它却不属于二次剩余．

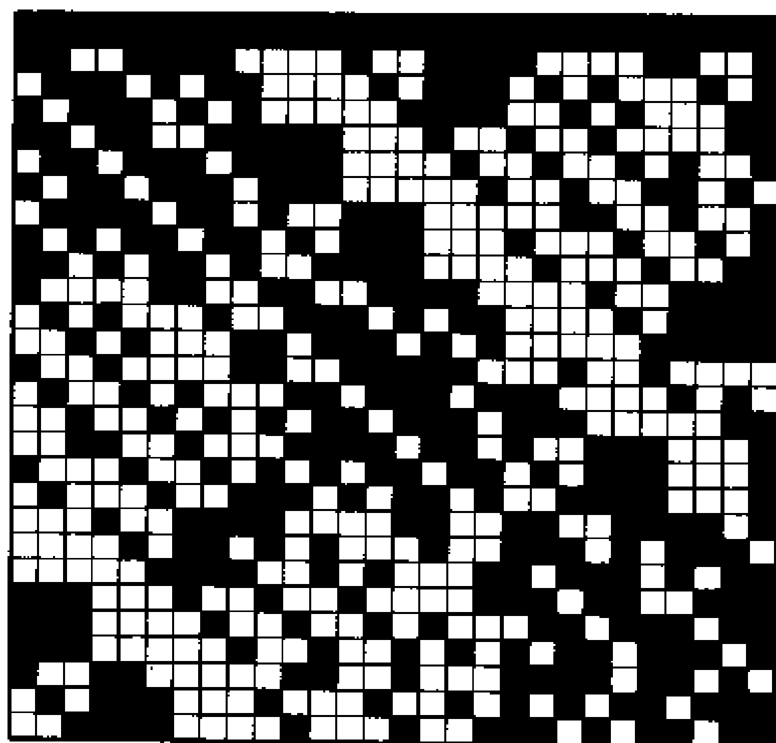
② 原著此段过于简略难懂．实际是先将序列$\{10^n, n=0,1,2,\cdots,27\}$作为 GF($3^3$)中的元并以 1021 为模化为$\{1,10,100,12,120,212,111,122,202,11,\cdots\}$．按一般数字大小排时即所谓“自然”顺序…….平方数实指由 10 的偶次方得来者．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



给出的①.后一位还给出了更复杂的法则，包括了 $m=2(p^n+1)$ 的情况，其中 p^n 具有 $4k+1$ 的形状.综合这些方法，他还解决了
[108] 如何构造一个具有 m^2 个网格的半条反拼砌，其中 m 能被 4 整除并可表示为 $2^k(p^n+1)$，p 是一个奇的素数.（当 $m=92$ 时，1961 年有人用别的方法藉助于电子计算机而解决了②.）



一个自反拼砌，$m=28$

图 4.3

在所有这些情况中的拼砌都有全是黑格子的一行还有全是黑格子的一列；因而每个别的行或列中的格子总是半数为黑的、

---

① Journal of Mathematics and Physics (Cambridge, Mass.), 1933, Vol. XII, pp. 311—320.实际上，佩利用的是减法而不是加法，不过由此而引起的变通是微不足道的.巴罗(J. A. Barrau)把这个理论很有趣地应用于 m 维几何学中，见 Nieuw Archief voor Wiskunde, 1906, series 2, Vol. VII.

② S. W. Golomb and L. D. Baumert, American Mathematical Monthly, 1968, Vol. LXX, pp. 12—17; Marshall Hall Jr., Combinatorial Theory, Waltham, Mass., 1967, p.207.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

半数为白的.当 m 是 4 的幂时,可以构造出一个"等色"的半条反拼砌,这里,等色的含义是指有半数的行和半数的列都是黑格比白格多 $\sqrt{m}$ 个,而其余的行和列都是白格比黑格多 $\sqrt{m}$ 个.本书第 10 版中给出了 $m=16$ 时的此种拼砌.

多米诺(超级骨牌) 1953 年戈隆(S.W.Golomb)提出了一种新奇的拼合问题①,不过,直到 Scientific American②的 1957 年 [109]
5 月号发行后才首次为广大公众所知.所谓多米诺是一种"超级骨牌"(或"多方联"),它们是由一些正方形沿边界接起来的接合片.多米诺通常又按它们的基本正方形的个数而分成不同的类别:单米诺只有一个单位正方形,双米诺就是由两个单位正方形接合成的长方形,三米诺就是由三个单位正方形顺次接合而成的东西.还可以推广到四米诺、五米诺、六米诺、七米诺、八米诺、九米诺、十米诺,等等,它们分别都是由四、五、六、七、八、九、十个单位正方形接合而成.如果两个 n 米诺不能经过平移、旋转或翻转而相互叠合,那么就认为它们是两个不同的 n 米诺.

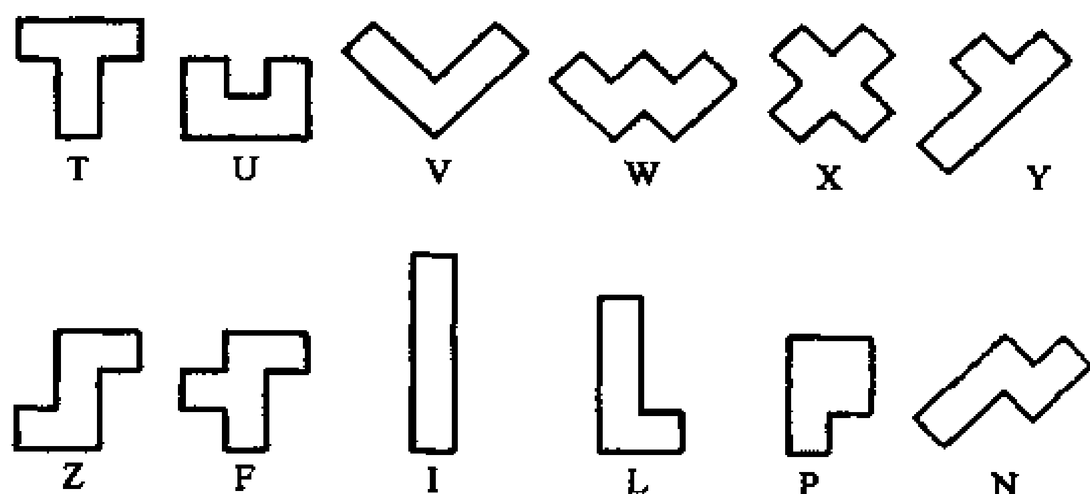


图 4.4

① S.W.Golomb, Polyominoes, New York, 1965.

② M.Gardner, Scientific American, 1957, Vol.CXCVI, no.5, pp.154—156; 1957, Vol.CXCVII, no.6, pp.151—159; 1969, Vol.CCXXI, no.6, pp.122—127.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

特别有趣的是五米诺①.它们共有 12 种形状,每一种大体上像一个英文字母;组合问题有:对于任一种五米诺,要求用其余 9 种五米诺拼成大小为该块三倍的相似图形;用同一种五米诺的复
[110] 制品拼成一个长方形(这只有 L,I,P,Y 四种五米诺是可能的);用 12 种五米诺块砌满除了一个指定的 2×2 正方形之外的棋盘.也可以用这 12 种五米诺砌成 3×20,4×15,5×12 或 6×10 的长方形.长方形 3×20 的砌法是唯一的,其法足以用序列 VZYWTFN-LIPXU 说明.可是对于 6×10 的长方形却有 2 339 种基本不同的砌法,这是哈兹尔格罗夫(C.B.Haselgrove)在英国曼彻斯特大学用计算机证明的.下图给出了 5×6 长方形仅有的两种砌法.

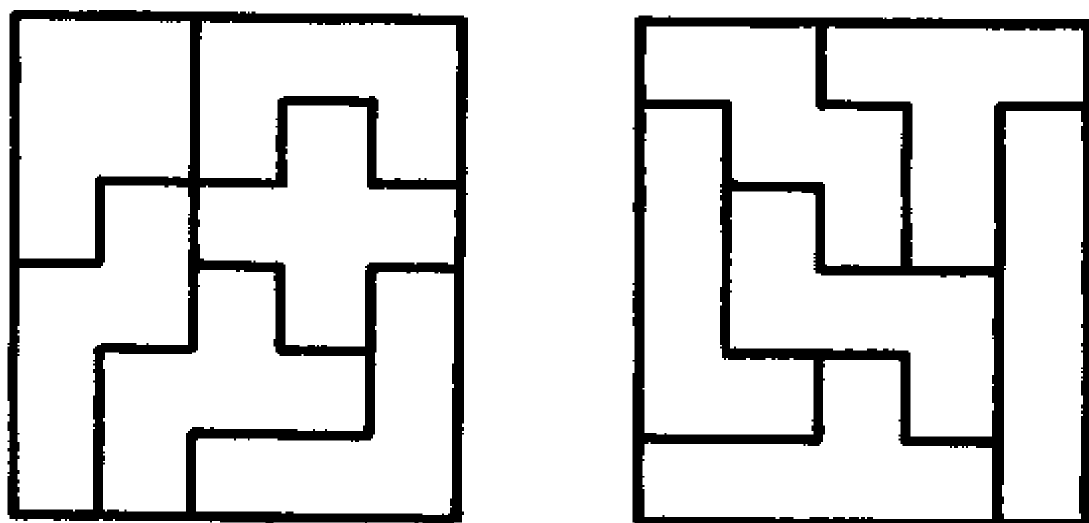


图 4.5

五米诺还可用以在棋盘上进行几种有趣的游戏,下边由戈隆所述的就是其中之一②.两个游戏人轮流往一个八行八列格

① 1919 年伦敦出版的杜德尼的书 The Cantebury Puzzles 里有关于五米诺的一个难题,即该书第 119—120 页上的问题 74:"破裂了的棋盘".

② 载于上述书中.或参看 M. Gardner, Scientific American, 1965, Vol. CCXIII, no.4, pp.96—104.菲利浦发行人制造了这个游戏的一套模块,叫做"盘凯"(*Pan-Kai*).

我们必须知道，而且我们必将知道

http://maths352.bokee.com

子的棋盘上每次下一块五米诺;直到有一个人(输者)无法再下而终局.此游戏颇能引人入胜,因为要想取胜需要很高的技巧和眼力.另一种不同的玩法是两家预先把所有的五米诺分定,然后开始下;这样一来,战术将相应地有所改变.

一个未解决的问题是寻求一个表达 n 米诺的不同的块数 [111]
$P(n)$的令人满意的公式.已经用计算机算出了当 n 较小时的一些 $P(n)$值;例如,下表中的数字就是几个人分头得到的结果:

n	1	2	3	4	5	6	7	8	9	10
$P(n)$	1	1	2	5	12	35	108	369	1 285	4 655

n	11	12	13	14	15	16
$P(n)$	17 073	63 600	238 591	901 971	3 426 576	13 079 255

首先考虑到 n 米诺的穷举问题的是伊登(M.Eden)①,他研究了函数 $P(n)$的增长率,其结果是当 n 充分大时$(3.14)^n < P(n) < (6.75)^n$.克拉纳(D.A.Klaner)②证明了$(P(n))^{1/n}$趋于极限$\theta$ 而$\theta > 3.72$.后来,克拉纳和里韦斯特(Rivest)③又证明了$\theta < 4.65$.于是,直到 1972 年,$P(n)$的最佳估计是$(3.72)^n < P(n) < (4.65)^n$.有人猜想比值 $P(n+1)/P(n)$随 n 的值而增大,据 $P(n)$的那些已知值而计算的结果看,这个猜想是对的.果其如此,则 $P(n+1)/P(n)$当 n 取任何自然数时的值都是θ的一个下界.例如,$n=15$ 时得到 $3.817 < \theta$,这对克拉纳的下界

---

① Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, 1961, Vol. IV, pp. 223—239.

② Canadian Journal of Mathematics, 1967, Vol. XIX, pp. 851—863.

③ "A procedure for improving the upper bound for the number of n-minoes"(改进 n 米诺个数的上界的一个方法), Canadian Journal of Mathematics, 1973, Vol. XXV, pp. 585—602.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

是一个很大的改进.

高维的 n 米诺也有人研究过.例如,已经计算出了当 $n \leqslant 7$ 时的三维 n 米诺的值 $P(n)$,如下表所示(如果两个立体的 n 米诺在反射变换下是全等的,那么要把它们看成是两个不同的 n 米诺.习惯上对于手套和鞋子正是这样:我们要区别"同一对"东西的左、右两只).

n	1	2	3	4	5	6	7	…
$P_3(n)$	1	1	2	8	29	166	1 023	…

有人提出了以此类三维 n 米诺为子块的三维难题.这些难
[112] 题(参看马丁·加德纳(Martin Gardner)的关于这个课题的论文①)中最通俗的是皮特·海因(Piet Hein)发明的所谓"立体拼装"或"索玛"(*Soma*)②.它包括 $n \leqslant 4$ 的一切非长方体的 n 米诺.这些子块的总体积是 27.问题之一是要把它们拼成一个棱长为 3 的正立方体.

加德纳的索玛立方体一文引起了许多读者对制作三维 n 米诺集合的极大兴趣.克拉纳把这些东西叫做 n 立方联,他造出了四立方联、五立方联和六立方联,并且解决了以这些立方联为子块的许多拼装问题.由 8 个四立方联所成的子块集合可用以拼成与这八者之一相似而棱长皆大一倍的四立方联,例如尺寸为 $2\times2\times8$ 与 $2\times4\times4$ 的长方体.从 29 个五立方联里去掉任一个之后,剩下的 28 个可以拼成尺寸为 $4\times5\times7$, $2\times5\times14$, $2\times7\times10$ 的各种长方体.布坎普(C. J. Bouwkamp)证明了此 $4\times5\times7$ 的长方体可以剖成一些子体,由原先的 28 种五立方联可以用 84 000 000 000 以上种不同的方式拼出这些子体来.尺寸为 3

① Scientific America, 1958, Vol. CXCIX, no. 3, pp. 182—188.

② "*Soma*"本指构成动物或植物躯体的细胞.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

×4×5的这些子体之一是由12个“平铺”五立方联(即12个立体的五米诺)拼成的.布坎普①还制备了由平铺的五立方联拼成3×4×5子块的所有拼法的一览表.实质上不相同的拼法共有3 940种.克拉纳曾经把166种六立方联拼成一个2×6×83的长方体,他还用去掉1×1×6的六立方联之后所剩的165种六立方联拼成五个尺寸为2×9×11的长方体.这些长方体又可以不同的方式组装成尺寸为9×10×11,2×9×55,2×11×55的各种长方体.还可以用144种六立方联拼成棱长为6的四个立方体.

彩色立方体问题

作为与拼砌类似的游戏的另一个例子,我要介绍彩色立方体问题②.避开数学的专门术语,这个问题可以叙述如下:一个立方
体有6个面,如果选取6种颜色,那么我们可以把各个面分别涂 [113]
上不同的颜色.调换涂色的次序,共得30种不同的彩色立方体.取这些立方体中的任一个,K;然后,要求从其余的29个立方体中选出8个来,把它们拼合成一个大立方体(它的每个棱长都是各个小立方体棱长的2倍),并且要这个大立方体表面上颜色的次序和K相同,而且任两小立方体相靠的面上的颜色彼此一样.

满足这些要求的8个小立方体只有一组.可以按下述规则去找出它们:取K的任一个面.它有四个角点.在每个角点处有三种颜色相邻.轮换这些颜色,对于每个角点我们得到另外两种立方体.这样总共得到8个立方体,它们就是要求的.稍加思索就会知道这一点,并且这个解答是唯一的.

---

① Catalogue of Solutions of the Rectangular 3×4×5 Solid Pentamino Problem. Technische Hogeschool, Eindhoven, The Netherlands, 1967.

② P. A. MacMahon, London Mathematical Society Proceedings, Vol. XXIV, 1893, pp. 145—155; New Mathematical Pastimes, Cambridge, 1921, pp. 42—46. 又可参看 F. Winter, Die Spiele der 30 bunten Würfel, Leipzig, 1934.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

例如，假定用字母 a,b,c,d,e,f 表示六种不同的颜色. 把立方体 K 放在桌面上，不妨认为底面的颜色是 f，顶面的颜色是 a，而东、北、西、南四个面的颜色分别是 b,c,d,e. 把这个安置记为 $(f;a;b,c,d,e)$. 将相会于东北上角的颜色作轮换则得立方体 $(f;c;a,b,d,e)$，再次轮换则得立方体 $(f;b;c,a,d,e)$. 相仿地，轮换 K 的会于西北上角的颜色，得立方体 $(f;d;b,a,c,e)$ 和 $(f;c;b,d,a,e)$. 再轮换西南上角的颜色得立方体 $(f;e;b,c,a,d)$ 和 $(f;d;b,c,e,a)$，又轮换东南上角的颜色得立方体 $(f;e;a,c,d,b)$ 和 $(f;b;e,c,d,a)$.

于是找到了 8 个所要的立方体. 要把它们拼合成一个和 K 的着色相同的大立方体而且相靠表面的颜色相同并不困难. 事
[114] 实上有两种拼合方法都满足上述条件. 一个方法是按上述立方体得到的次序把第 3,6,8,2 个立方体依次放到 K 的底面的 SE（东南）、NE（东北）、NW（西北）和 SW（西南）角，当然啰，要每个立方体的 f 面都向下，这时第 3 和第 6 个立方体的 b 面都要向东，第 2 和第 8 个立方体的 d 面都要向西. 再把第 7,1,4,5 个立方体依次放在 K 的顶面的 SE（东南）、NE（东北）、NW（西北）和 SW（西南）角；当然啰，要每个立方体的 a 面都向上，这时第 7 和第 1 个立方体的 b 面都要向东，第 5 和第 4 个立方体的 d 面都要向西. 如果 K 没有给定，问题的困难有所增加. 也可以提出类似的二维难题.

剖矩成方　莫龙（Z. Moroń）①曾观察到有一组 9 个不等的正方形可以拼合成一个 32×33 的长方形. 这是一个诱人的研究问题的起源，有时称之为"拼方成矩". 当一个正方形或长方形可以被剖分成一些不相等的正方形时，称之为"完全的". 这些剖得的正方形为它的"元"，元的个数为它的"阶". 如果它不包含较小的

① Przeglad matematyczno – fizyczny, Warsaw, 1925, Vol. III, pp. 152—153.

我们必须知道，而且我们必将知道

完全长方形,那么称它为“简单的”,否则称它为“复合的”.已经用“经验法”得到许多完全正方形,这方法就是先作出一个完全长方形一览表,然后试着把它们之中的一些往一块拼合,可能在角上空着一些正方形.斯普拉格(R.Sprague)①用这个办法得到了一个55阶的完全正方形.相仿地,布鲁克斯(R.L.Brooks)、史密斯(C.A.B.Smith)、斯通(A.H.Stone)、塔特(W.T.Tutte)②得到一个26阶的完全正方形.这些作者们还阐述了一个“理论的方法”,可以用它造出39阶以及更高阶的完全正方形.威尔科克斯(T.H.Willcocks)③给出了一个“经验的”24阶完全正方形,这是已知的最低阶的完全正方形,它的元是1,2,3,4,5,8,9,14,16,18,20,29,30,31,33,35,38,39,43,51,55,56,64,81.现在在组合数学期刊(Journal of Combinatory Mathematics)每一期的封面上都画着它.费德里科(P.J.Federico)④造出了另一些低阶的完全正方形.这两位作者曾修正了“理论方法”而获得直到31阶的完全正方形.“经验而得 [115]
的”完全正方形是复合的.威尔逊(J.C.Wilson)用计算机进行研究⑤,曾经找到一个25阶的简单完全正方形.布坎普、杜伊维斯蒂茵(A.J.W.Duijvestijn)、米德马(P.Medema)已造出由9到15阶的简单完全长方形表⑥.借助于计算机的搜索,他们已发现没有低于20阶的简单完全正方形.

1968年布鲁克斯(R.L.Brooks)发现了第一个简单的完全长方形,其边长之比为2:1.它的阶数是1323.此后,费德里科发展了一个“经验法”,由此得出了一些阶数低得多的边长之比为

---

① Mathematische Zeitschrift,1939,Vol.XLV,pp.607—608.

② Duke Mathematical Journal,1940,Vol.VII,pp.312—340.

③ Canadian Journal of Mathematics,1951,Vol.III,pp.304—308.

④ 前刊,1963,Vol. XV, pp. 350—362.

⑤ W.T.Tutte, American Mathematical Monthly,1965,Vol.LXXII,pp.29—35.

⑥ Technische Hogeschool, Eindhoven, 1960.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

2 比 1 的简单完全长方形，在有些情况下，低达 23.

动态的布局游戏

用棋子在各种棋盘上走动的游戏更为有趣，例如，跳棋、狐鹅棋、单人棋、双陆棋、象棋、西洋棋. 一般地说，由于棋子的许可走步太多而难以作数学的分析. 不过在少数游戏中棋步的限制较严因而可作数学的处理，后边将给出一两种例子. 这里我限于主要介绍难题和简单的游戏.

调车问题 头一个我要说的是数年前我花钱学来的一个小游戏，叫做“大北方难题”. 它是许多有关火车调度的一个有代表性的问题. 我拿它作为一个典型，虽然其中的假设很不现实.

问题里给出一段铁路 *DEF* 和两股岔道 *DBA* 与 *FCA*，二者在 *A* 处汇合. 汇合后的一段铁轨的长度仅足停一辆车箱，例如 *P* 或 *Q*，它们都可以进入或开出 *A* 段；但这段铁轨较一辆机车
[116] (如 *R*)为短，因而整辆机车不能全部开到 *A* 段铁轨上. 所以，如果一辆机车开上某一岔道(如 *DBA*)后，要回到干线上的话必须沿原岔道退回.

开始时，用一小块染了色的木头 *P* 代表一辆车箱，放在 *B* 处；另一段染色不同的木头 *Q* 代表另一辆车箱，放在 *C* 处；还有一段较长的木头 *R* 代表一辆机车，放在 *E* 处. 问题要求利用机车 *R* 拖动车箱使 *P* 与 *Q* 换位而无需使用机动岔道.

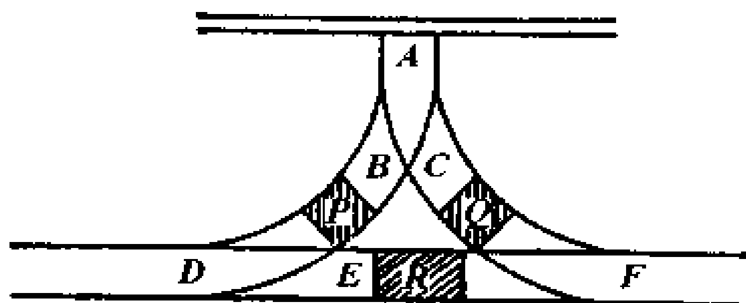


图 4.6

我们必须知道，而且我们必将知道

http://maths352.bokee.com

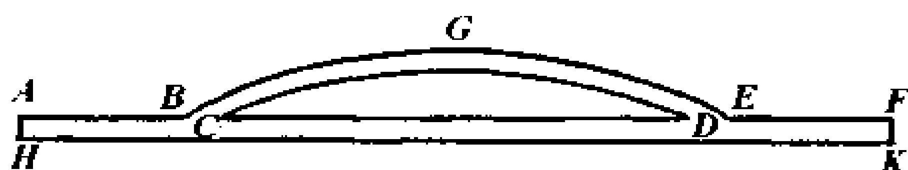


图 4.7

1905 年街头上经营的另一调车游戏叫做"奇夫切马尔波(Chifu – Chemulpo)难题"①.是这样的:一条侧线 BGE 在点 B 和点 E 处与铁路正线 AF 相汇.假定这正线的两端 A 与 F 都已被堵塞了,如图 4.7 所示.在这个游戏的模型里,铁路 AF 长为 9 寸,$AB = EF = 1\frac{5}{6}$ 寸,宽 $AH = FK = BC = DE = \frac{1}{4}$ 寸.有八辆车箱和一辆机车的模型,长度都是 1 寸,宽度都是 $\frac{1}{4}$ 寸.车箱上有编号 1 至 8.开始时,机车停在侧线上,八辆车箱都停在正线上,按 1,2,3,4,5,6,7,8 的次序由 A 向 F 排列.任何时候正线上停的车都不可能多于 8 辆.如果正线上有 8 辆车,那么只有从任一头数的第二辆车能够进入侧线.如果正线上停的车数少于 8 辆,那么任一端的两辆车都能进入侧线.如果侧线两端接轨处皆无车,那么正线上只能停 4 辆车而不能多于 4 辆,这时侧线上应有 [117]
5 辆车箱或者 4 辆车箱和 1 辆机车.问题的要求是颠倒正线上的车箱的次序,使车上的号码由 A 向 F 数时是由 8 到 1,并且要机车和车箱上下侧线的次数尽可能地少.26 步是需要的,并且 26 步的解法不只一个(参看本章附录).

其他调车问题也并非不通俗,不过这两个例子也够了.

摆渡问题 大家都熟悉这个故事:一位卖艺的携带着一只狼、一只羊和一篮子白菜在旅途中遇到一条河,唯一的渡河工具是一条小船.它只能载他自己和所带的三样东西之一.显然他不

---

① 在中国也有这种游戏,通常就叫做"错车问题",但未作经营.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

能把狼和羊留下，也不能把羊和白菜留下．问题是他们怎样才能安全地渡过河去?[①]

一个类似的问题是要求安排三个人和三个小孩渡河．他们只有一条船，它每次至多只能载一个大人或两个小孩．至少要往返 15 次[②].

中世纪的作家如阿尔昆、塔尔塔利亚等人提出过许多此类问题．下边是这种问题的一个常见的典型．三个[③]美丽的夫人和她们的丈夫一同旅行．三位先生都很年轻、殷勤而又心怀猜忌．他们来到了一条河边，要想过河但只有一条至多仅能载二人的小船．于是约定，除非自己的丈夫在身旁，任一女士不得和男人们在一起．问怎样安排渡河的步骤？答案需要往返 11 次．如果只有两对夫妇，那么往返 5 次就够了．如果有四对夫妇，那么问题是无法解决的．

[118] 另一个问题是 n 对夫妻用一条船过河，该船可载至多 $n-1$ 个人，条件仍是任一女士除非自己的丈夫在身旁不得和别的男人在一起．上述阿尔昆问题是这个问题当 $n=3$ 时的特例．令 y 表示渡河需要往返的次数．已经证明 $n=3$ 时 $y=11$；$n=4$ 时 $y=9$；$n>4$ 时 $y=7$.

下边的类似问题是吕卡斯[④]提出的．问一条渡船最小须能载几人才能使 n 对夫妻可乘它渡河而任一女士除非自己的丈夫在身旁不得和别的男人在一起；任何一个人都能够划该船．此外还要求往返摆渡的最少次数 y．德兰努瓦(M. Delannoy)证明了当 $n=2$ 时 $x=2$ 而 $y=5$；当 $n=3$ 时 $x=2$ 而 $y=11$；当 $n=4$

① Ozanam，1803 年版，Vol. Ⅰ，p.171；1840 年版，p.77.

② H.E.Dudeney，The Tribune．October 4，1906.

③ Bachet，附录，问题 Ⅳ，p.212.

④ Récréations mathématiques，Paris，1883，Vol. Ⅰ，pp. 15—38，237—238．以后提到此文时仅指出作者姓名．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

时 $x=3$ 而 $y=9$；当 $n=5$ 时 $x=3$ 而 $y=11$；最后，当 $n>5$ 时 $x=4$而 $y=2n-3$.

德·丰特内(M. De Fonteney)曾指出，如果河中有一个岛，那么只要有一条可以乘坐两个人的小船，就总可以把所有的夫妻都摆渡过去：如果只有两对或三对夫妻，岛是不必要的，这两个情况已经概括在前述方法里了.他的解答需要 $8n-6$ 次摆渡如下：不管有几对夫妻，前 9 次摆渡都是一样的，其结果是把一对夫妻送到岛上而另一对夫妻送到对岸.往后每 8 次摆渡的结果都把一对夫妻由此岸送到了彼岸；直到还有一对夫妻尚留在此岸、另一对夫妻已在岛上，其余的人都已达彼岸.最后 7 次摆渡把所有剩下的两对都送到对岸.然而，如果 n 大于 3，似乎不 [119]
需要多于 $6n-7$ 次的摆渡①.

塔里(M.G.Tarry)曾提出问题的一个推广，使它的解更为复杂.他假定每个丈夫带着 m 个妻妾旅行；此外，因为回教徒的妇女都是在深闺中长大的，所以有理由假设她们在没有一个男子的帮助下是不会划船的.不过对于基督教徒来说，带着一个妻子而旅行所遇到的困难也是很大的.这里我只用提到回教徒在类似的情况下遇到的更多的麻烦就够了.

测地线 涉及曲面上由一点到另一点的最短路线的几何问题通常是困难的，但是在一个或几个平面上的测地线一般地并不难确定.

我附带举一个例子②.要不是亲自见到过一些读者不能马上看出答案来，我会犹豫要不要举这个例子的.问题是这样.有

① 参看 H.E.Dudeney, Amusements in Mathematics, London, 1917, p.237.

② 这个例子是杜德尼先生提出的.1903 年我在剑桥听到过一个类似的问题，但第一次看到它的发表是在伦敦的 Daily Mail 的 1905 年 2 月第 1 号上.

我们必须知道，而且我们必将知道

[redacted]

一个长 30 呎、宽 12 呎、高 12 呎的房间. 在较短一边墙壁的竖直平分线上离天花板 1 呎处有一只捕蝇虎①. 在对面墙壁的竖直平分线上离天花板 11 呎处有一只苍蝇. 捕蝇虎要捕食这只苍蝇而悄悄地向它爬过去,苍蝇一看到它就吓呆了. 问捕蝇虎应采取的最短路线是什么?

为了寻求答案,请注意我们可以剪出一片纸来,使它经过适当的折转之后恰好成为和这个房间相似的模型. 这个纸模型可以有几种不同的剪法. 如果当把纸片摊平之后我们能够用完全落在纸片内的直线把代表捕蝇虎的点和代表苍蝇的点连起来,那么我们就得到它们之间的一条测地线(最短路径)了. 于是问
[120] 题归结于如何剪出这种纸片.

图 4.8 所示就是上述问题的解法之一,其中 A 代表地板,B 和 D 代表较长的两面墙,C 是天花板,W 与 F 分别代表捕蝇虎与苍蝇原先所在的位置,它们之间的距离的平方是 32^2+24^2,所以距离是 40 呎.

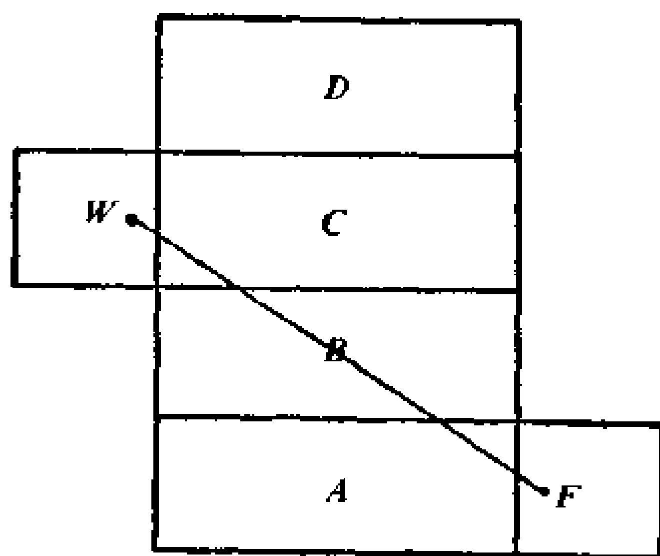


图 4.8

① 一种形似蜘蛛善捕食蚊蝇的小虫. ——译者注

http://maths352.bokee.com

单行棋子游戏 许多动态的游戏和问题都可以用一盒棋子来说明，特别是那些具有两种颜色的棋子的游戏．当然，硬币也好、卒子也好、纸牌也好，都一样可用．以下我来叙述几个此类游戏．

问题之一 我的读者们对这个问题一定是很熟悉的．十个棋子(或者硬币)排成一行．可以把任一个棋子跳过两个相邻的棋子而摞到第三个上去．要求按这个规则把它们走成距离相同的五摞．

如果把它们原先的位置记为1,2,3,4,5,6,7,8,9,10，那么可以这样走：把7上的棋子摞到10上，然后把5上的棋子摞到2上，然后3到8上，1到4上，最后把9上的棋子摞到6上．于是这十个棋子变成两个一摞，分别位于原来的第2,4,6,8,10号位置上了． [121]

相仿地还可以把4上的棋子摞到1上，然后6到9上，8到3上，10到7上，最后2到5上．于是它们也是五摞，但分别位于原来的第1,3,5,7,9号位置上．

如果把两个摞在一起的棋子算做一个，那么和上述类似的解是：7到10上，然后5到2上，3到8上，1到6上，最后9到4上；或者先把4号位置上的棋子摞到1号位置的棋子上，然后6到9上，接下去8到3上，10到5上，最后2到7上①．

还有一个用8个棋子玩的类似的游戏，不过最后摞成的四对的位置不再是等距离的了．走法是先把5号位置上的棋子摞到2号位置上的棋子上，然后3到7上，4到1上，最后6到8上．这样的游戏完全可以推广到用$8+2n$个棋子去玩，因为只要把4号位置上的棋子摞到1号位置上的棋子上，那么就只在这一摞的左边还剩下$8+2n-2$个棋子尚待解决．同样的走法

① 本书第3版法文译本(Paris, 1898)上由菲茨帕特里克(J. Fitz-patrick)所给的注记．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

又可以把问题化至 $8+2n-4$ 个棋子的问题，如此下去，直到只剩下左边的 8 个棋子，它们可以按上述走法解决.

一种更一般的推广是用 n 个棋子做游戏①，走法是任一棋子可以越过 m 个相邻的棋子而摞到第 $m+1$ 个上去. 例如，把 12 个棋子排成一行，每步要越过 3 个相邻的棋子. 这样可以走成四摞，每摞 3 个棋子. 为此，先把棋子依次编写上号码. 走法之一是：7 到 3，然后 5 到 10，9 到 7，12 到 8，4 到 5，11 到 12，2 到 6，1 到 2. 或者把 16 个棋子排成一行，每步要越过 4 个相邻的棋子. 这样可以走成 4 摞、每摞 4 个棋子. 走法之一是：8 到 3，然后 9 到 14，1 到 5，16 到 12，7 到 8，10 到 7，6 到 9，15 到 16，13 到 1，
[122] 4 到 15，2 到 13，11 到 6.

问题之二　另一个大体相仿的游戏源于日本②. 把 4 个白棋子（或面值五分的硬币）和 4 个黑棋子（或面值一分的硬币）交错相邻地排成一行. 走法是每步要走两个相邻的棋子并且不许改变它们的相互位置. 要求用 4 步把它们变成新的一行，这时 4 个黑子全在前边、4 个黑子全在后边，彼此相邻而无空档.

这个问题可以这样解决. 用 a 表示白子，b 表示黑子，×× 表示两个相邻的空位，则这些棋子在每走一步之后的相继位置可以表明如下：

未走之前	× × *abababab*
走一步之后	*baababa* × × *b*
走两步之后	*baab* × × *aabb*
走三步之后	*b* × × *baaaabb*
走四步之后	*bbbbaaaa* × ×

走法是以下列规则为依据的. 假定棋子原先排成一个圆环，它有

① n 不能取为素数，m 须是 n 的因子. ——译者注

② La Nature, June, 1887, p.10.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

两个相邻的空档.在每次走步时总是把空档的固定一侧的隔一个和隔两个位置的那两个子走到两个空档位置上.

自然可以提出有 $2n$ 个棋子的相仿的问题,其中有 n 个是白子,另 n 个是黑子.如果 n 大于4,可以经过 n 步走子而得以解决.不过,我未能找到一个概括所有类似情况的简单规则.不过,德兰努瓦给出了当 n 等于 $4m$,$4m+2$,$4m+1$ 或 $4m+3$ 时的解法①,在前两种情况下,前 $\frac{1}{2}n$ 步都是移动两个不同色的棋子,后 $\frac{1}{2}n$ 步中每步都移动两个同色的棋子;在后两种情况下,第一步与上边所给出的走法一样(即,先走倒数第二子与第三子),然后 [123]
的 $\frac{1}{2}(n-1)$ 步走的都是两个不同色的棋子,最后的 $\frac{1}{2}(n-1)$ 步走的都是两个同色的棋子.

如果我们取消每次拿起来的两个棋子必须移送到行列的两端之一这个限制,而代之以最后的行列必须是无空档的,那么问题仍是可解的.

泰特提出过问题的一个不同的提法.他要求要走的两个棋子必须先交换位置.这种提法的问题当棋子为四对时似乎需走五步,在一般情况下需走 $n+1$ 步.

一盘棋子游戏　下边的三个问题既要使用两种颜色的棋子,又要用到棋盘.用卒和兵比别的什么筹码更方便些.我在叙述中如果使用卒和兵二字只是为了说话方便而不是和象棋有什么联系.第一个问题的特点是棋子在任何位置至多有两种步子可走,第二个和第三个问题中的棋子在任何位置上至多只有四种步子可走.在这种限制下,可以进行分析.我不打算讨论允许

① Bibliotheca Mathematica, 1896, series 3, Vol. VI, p. 323; P. G. Tait, Philosophical Magazine, London, January, 1884, series 5, Vol. XVII, p. 39; 或 Collected Scientific Papers, Cambridge, Vol. II, 1890, p. 93.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

更多种步子的类似问题.

兵卒问题之一　在棋盘的某一行 7 个相连的方格上，一端摆上 3 个白子(或兵)，在图中记为 3 个 a，另一端摆上 3 个黑子(或卒)，在图中记为 3 个 b，中间的一个方格空着. 每个棋子只能向一个方向走：a 只能由左向右走，b 只能由右向左走. 如果一个棋子
[124] 和一个空格相邻，那么它可以走进空格；如果一个棋子和一个不同颜色的棋子相邻而后者和一个空格相邻，那么前者可以跳进那个空格里. 问题的要求是将所有的白子与所有的黑子调换位置.

a	a	a		b	b	b

图 4.9

解答需 15 步. 先走 1 个白子，然后接连走 2 个黑子，再走 3 个白子，再走 3 个黑子，再走 3 个白子，再走 2 个黑子，最后走 1 个白子. 如果用数码将 7 个方格的位置依次序编号，那么上述解答可以表示为如下的过程：空格开始时的位置是 4，然后逐步的变动位置是 3，5，6，4，2，1，3，5，7，6，4，2，3，5，4. 这些走步之中有 6 步是平移、9 步是跳越.

更一般的问题是，一行有 $m+n+1$ 个方格，一端放上 m 个白子，另一端放上 n 个黑子. 经过 $mn+m+n$ 步可以把白子走到黑子原先所在的一端而黑子走到白子原先所在的一端，其中有 $m+n$ 步是平移，mn 步是跳越.

a	a	a	a	b	b	b
a	a	a	a	b	b	b
a	a	a	a	b	b	b
a	a	a		b	b	b
a	a	a	b	b	b	b
a	a	a	b	b	b	b
a	a	a	b	b	b	b

图 4.10

我们必须知道，而且我们必将知道

http://maths352.bokee.com



兵卒问题之二① 一种类似的游戏可以在长方形或正方形的棋盘上玩.用具有 49 个方格的正方形棋盘足以说明此类游戏的玩法.图 4.10 表明了开始的阵势,其中的 a 代表兵或白子、b 代表卒或黑子.a 可以从左向右或从上向下走,b 可以从右向左或从下向上走,走或跳的规则如前. [125]

解答归结于前述问题之一的情况.中间一行的棋子可经 15 步左右换位.在此过程中总有一列它包含着一个空格,这时就可以把这一列中的棋子上下换位.7 行中每一行的左右换位都需

我们必须知道，而且我们必将知道

http://maths352.bokee.com

黑色粗线所围的容许区域.

由于棋盘上容许区域内只有一个方格是空着的,并且不准
[126] 沿对角线方向走,也不准后退,所以每次走动时,两种颜色的子共有四个可以走动.然而,经验得到的解法很多.下边是杜德尼先生给出的解法,共46步:

*Hhg * Ffc * GBHh * GDFfehbag * GABHEFfdg * Hhbc * CFf * GHh **

字母或星号表示相继走动的子所占的方格①.注意走完前23步时得到的是一个对称的阵势,后22步的走法可以由按倒序写出前22步再将大写字母换成同名的小写字母并把小写字母换成同名的大写字母而得到.不难构成各种形状的棋盘上的问题.

如果不厌其烦的话,像上边列举的游戏的数学理论恐怕是可以利用范德蒙特(A.T.Vandermonde)的记号(见后边第6章)或用类似于单人象棋理论②中所用的方法予以阐述的.

下棋问题 除了兵卒两种棋子之外,还有些多种棋子的数学游戏.在第6章里给出一些下棋的问题.

立 交 环

想象某些简单图形的几何变化有时并非容易的事.这可以用众所周知的立交环来证实.它是由一个纸圈按下述方式剪出的:

取一个纸条或一段纸带子(为了方便,不妨假定它有一两寸宽,至少十多寸长),沿纸条的中线画一直线 AB,把 A 端和 B 端黏到一起,我们得到一个环子,就像从一个柱面上截下来一段似的.如果把这个纸环沿中线剪开,我们将得到两个完全相同的两

① 这里把字母或星号都当作方格的名称.譬如第4步 * 表示 * 格上的子走或跳.——译者注

② 关于单人象棋的理论,参看 Reiss, "Beiträge zur Theorie des Solitär-Spiels," Crelle's Journal, Berlin, 1858, Vol. LIV, pp.344—379;以及 Lucas, Vol. Ⅰ, part Ⅴ, pp.89—141.

我们必须知道，而且我们必将知道

个纸环,只不过每个环的宽度是原来的一半.其次假定在把 A,B 两端黏合之前先把 A 端扭转两个直角,然后再黏合起来,其结果是 A 端的背面与 B 端的正面黏合.这时再沿中线剪开将只得到一个纸环.然后再假定在把 A,B 两端黏合之前先把 A 端扭转一周(即,转过四个直角),这时沿中线剪开后得到两个相互套 [127]
在一起的环子.如果我的读者们中有谁认为这些结果可以不假思索地预先断定,那么请看看他自己是否能够正确地预言把上述第二次和第三次得到的结果再沿中线剪开后得到些什么来,这可能对他是很有趣的.

这方面的理论属于利斯廷(J. B. Listing)与泰特(P. G. Tait)①,他们讨论了在把 A,B 两端黏合之前先将 A 端扭转 m 个平角($m\pi$),然后再黏合的各种情况.

若 m 为偶数,黏成的是具有正反两面和两条边的一个纸环.如果把这个面沿中线剪开,我们将得到两个纸环,每个都扭转 m 个半圈,两个环子相互套结 $\frac{1}{2}m$ 次.

若 m 为奇数,黏成的是仅有一个面和一条边的一个纸环.如果把它沿中线剪开,我们将只得到一个纸环,它扭转 $2m+2$

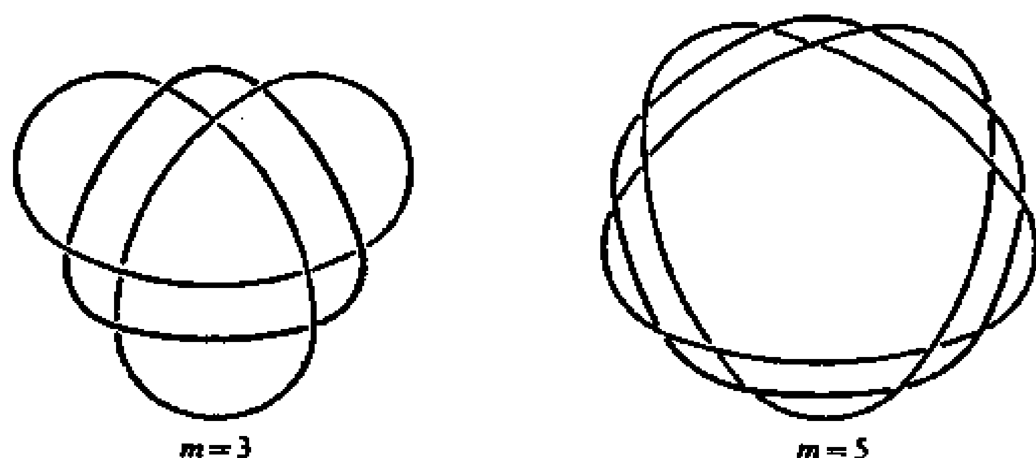


图 4.12

① Vorstudien zur Topologie, Göttinger Studien, 1847, part X.

http://maths352.bokee.com

个半圈，并且当 m 大于 1 时，它是扭结的．如果不是把纸环沿中线剪为两个，而是剪成三等分①，我们会得到两个相套在一起的环子：一个和原来的一样（来自中间的那一条），另一个和二等分所得的一样．这两个环子的扭结方式有如图 4.12 所示（$m = 3$ 和 $m = 5$ 两种情况）．当 $m = 1$ 时，环子称为“麦比乌斯（Möbius）
[128] 带”．

附　　录

Ⅰ．对 108 页的补注　文中所说将16个棋子排在15条直线上的排法如下：一个正五边形的五条对角线相交的交点构成第二个小正五边形的顶点．这个小正五边形的对角线相交的交点又恰是第三个更小的正五边形的顶点．这三个正五边形的 15 个顶点和它们共同的中心就是所要求的点阵（Dudeney's Canterbury Puzzles，1919，p.175）．

将 18 个棋子排成 9 行、每行 5 个棋子，排法如下：从一个等边三角形 $AA'A''$ 的顶点之一，A，向三角形内引直线 AD，AE，它们与 AA' 的夹角可以是大于零而小于 60 度的任何值．再从顶点 A' 与 A'' 各向三角形内引直线 $A'D'$，$A'E'$ 与 $A''D''$，$A''E''$，它们与 $A'A''$，$A''A$ 所成的角和 AD，AE 与 AA' 所成的角分别相同．记 $A'D'$ 与 $A''E''$ 的交点为 F，$A'E'$ 与 $A''D''$ 的交点为 G，则 AFG 成一直线．三角形的 3 个顶点和 AD，AE，AF 与由 A'、A'' 各引出相仿的两束直线相交所得 15 个交点构成所求的点阵．

将 19 个棋子排成 10 行，每行 5 个棋子．这种安排可以将棋子放在 10 条直线 $x = \pm a$，$x = \pm b$，$y = \pm a$，$y = \pm b$，$y = \pm x$ 交点上而得出，不过这时有两个交点被认为在无穷远处．

再举一个例子．考虑怎样把 28 个棋子排成 36 行，每行 4 个棋子．这可以把一个正九边形 $A_1A_2\cdots A_9$ 的某些顶点用直线连

① 这个注说是安德烈斯（J.M.Andreas）给出的．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

起来而得到另外两个九边形 $B_1B_2\cdots B_9$ 和 $C_1C_2\cdots C_9$，它们都和原来的九边形有着一个共同的中心．B_1 是 A_3A_6 与 A_5A_8 的交点，C_1 是 A_2A_5 与 A_5A_9 的交点．直线 B_4B_7 通过 C_5 和 C_6．第 28 点是中心点，有 9 条直线通过它，例如 $A_1B_1C_1$．

Ⅱ．对 120 页的补注 大北方调车难题解法如下：(i) R 将 P 推到 A；(ii) R 返回原处，再把 Q 推上去使 P 与 Q 挂钩，然后把它们拉到 E；(iii)将 P 脱钩①，再用 R 将 Q 推回 A，把它留在那里；(iv) R 回来将 P 挂上送到 C，把 P 留在 C；(v) R 相继经过 F，D，B 而开到 A，再把 Q 拉出来，留于 B 处．

Ⅲ．对 121 页的补注 奇夫切马尔波难题的解法是：相继把 2，3，4 号车箱送上去，即，送到侧线上．〔然后把 1 沿正线推近 5；这不算"一步"．〕然后，4 下来，即，送到正线上靠近 1．然后，8 上去，3 下来到正线一端暂停在那里，6 上去，2 下来，机车下来，3 上去，7 上去．〔然后把 5 推到正线的一端暂停在那里．〕然后，7 下来，6 下来，2 上去，4 上去．〔然后机车开到 1．〕然后 4 下到正线一端，暂停在那里，2 下来，5 上去，3 下来，6 上去，7 上去，8 下到正线一端，机车上去，5 下来，6 下来，7 下来．在这个解里，机车开到正线的一端，然后可以沿正线行驶，最后从正线的另一端开到侧线上．也完全可以把机车开到正线的一端，最后就从该端开到侧线上去．在这个解里，用 e 表示机车，则车辆被调动的顺序是 2，3，4，4，e，8，7，3，2，6，5，5，6，3，2，7，2，5，6，3，7，e，8，5，6，7． [129]

① P 要留在 E 处．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第5章 多面体

“空间物体的讲述为几何学中不常见甚至往往被忽视的部分.然而那些对于科学的实在领域和思辨领域有同样爱好的才智之士无疑会认为它并非不足道或无益的增补.对于他们来说,思辨领域是兴趣的主要所在.”①

多面体是一种立体物②,它的表面都是平的、它的棱都是直线段,而每条棱都是它的两个顶点的连线,同时又是它的两个面的公共边.常见的例子有棱锥和棱柱.(五角棱锥有6个顶点、10条棱、6个面;五角棱柱有10个顶点,15条棱、7个面.参看图5.1中的第7图.)我还要提一下*反棱柱*③,它的两个底面虽然是平行的,但是相对位置不一样,每个顶点对着另一底面的一个边,因而侧面上的棱连接成封闭的折线.(一个五角反棱柱有10个顶点、20条棱、12个面.参看图5.1中的第9图.)

前一章里介绍的拼砌可以看成是无穷多面体.

对称性与对称体

如果一个图形能够和它在平面镜里的象的图形相叠合(用

---

① Abraham Sharp, Geometry Improv'd, London, 1717, p. 65.

② 确切地说,它是这种立体物的表面.

③ 或“拟棱柱”.见大英百科全书(第十四版)“Solids”条.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

最通俗的话来说，即它是“对称的”），那么最好说这个图形是自反射的①．一个非自反射的图形和它的镜象构成一个配对．（明 [130]
显的例子如一对鞋．）一个自反射的图形至少有一个对称平面，它在这个平面里照出的图形和原来的完全一样．一个图形还可以具有绕一个对称轴作旋转时不变的对称性．说某个图形具有一些对称性，这句泛泛的话可以说得更为确切一些——该图形在一些对称变换下不变．对称变换②被定义为使图形不变的运动与反射的任何组合．

对于一个正多边形 $ABC\cdots X$，有一个对称（事实上是一个转动）它把所有的顶点进行轮换：把 A 变至 B，B 变至 C，…，X 变至 A．

五个柏拉图体③

令 A 为一多面体的任一面 α 的任一顶点．如果这多面体具有那样两种对称性：一是轮换 α 的顶点，另一是轮换围成 A 的各个面，那么这个多面体就称为正多面体．于是所有的面都是正多边形而且彼此大小相等，所有的棱长也都相等，并且所有的顶点都同样地布绕在这多面体的表面上．如果每个顶点都与 q 个 p 边形相邻，我们可以用符号 p^q 或 $\{p,q\}$ 记这个多面体．

如果多面体是有限的④，那么汇于同一个顶点的所有的面形成一个立体角．每个面的内角是 $(p-2)\pi/p$，所以 $q(p-2)\pi/p<2\pi$，即

$$(p-2)(q-2)<4.$$

由于 p 和 q 都大于2，我们只需考虑两个正整数的乘积为1，2

① 或“自反射的”．

② 或“对称”．（任一迁移或旋转皆可视为两次相继的反射．）

③ 柏拉图体（Platonic Solids）即正多面体．——译者注

④ 面与面数皆有限．——译者注

我们必须知道，而且我们必将知道

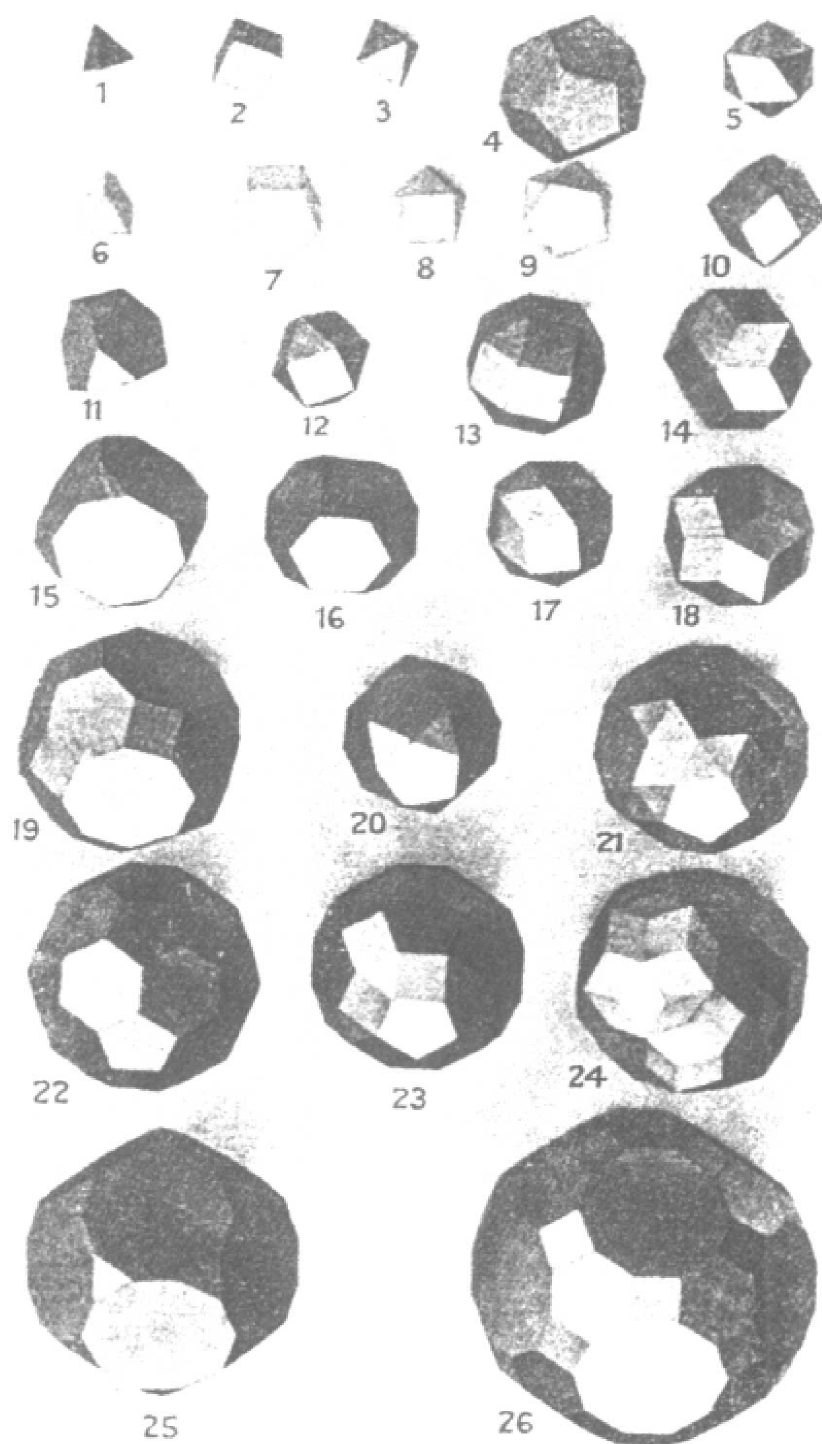


图 5.1

我们必须知道，而且我们必将知道

http://maths352.bokee.com

或 3 的可能结合方式，然后就可以在每种情况下一个面一个面地拼成多面体来.令 V,E,F 分别表示顶点数、棱数、面数，则结果载于下表中.(参看图 5.1 中的第 1,2,3,4,5 图.) [131]

$\{p,q\}$	V	E	F	名　称
$\{3,3\}$	4	6	4	正四面体
$\{4,3\}$	8	12	6	正立方体
$\{3,4\}$	6	12	8	正八面体
$\{5,3\}$	20	30	12	正十二面体
$\{3,5\}$	12	30	20	正二十面体

显然，$qV=2E=pF$.一个不太明显的关系是

$$E^{-1}=p^{-1}+q^{-1}-\frac{1}{2}.$$

它很容易从第 8 章里证明的欧拉公式 $F+V-E=2$ 推出来.

正四面体可以按四种不同的看法把它看成一个三角锥①，正八面体可以看成三角反棱柱，它还可以按三种不同的看法看成双四棱锥，正立方体可以看成四棱柱.正二十面体可以按六种不同的看法看成五角反棱柱，柱的上、下底各黏上一个正五棱锥.正十二面体可以看成是由两个平行平面上的正五边形——它们各自的每个边都与另 5 个同样大的正五边形相邻接——二者嵌合而成的.

一个正二十面体可以内接于一个正八面体，这正二十面体的每个顶点皆按“黄金分割”②分截该正八面体的一个棱.一个正立方体可以内接于一个正十二面体，这正立方体的每条棱分别含于该正十二面体的一个面内并且是该面的一条对角线.

自古以来这五种形体就为人所知.最早对它们进行彻底研究

① 原文称三角形三棱锥，略去赘字，下同.——译者注

② 参看本书第 57 页.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的人可能是西艾泰德斯(Theaetetus)[①].有人猜想欧几里得最初写他的《原本》时并不是要写一本几何学通论而是想为彻底了解这五种正多面体而铺平道路.不管怎么说,欧几里得以正三角形
[132] 的作图开始而以正十二面体的作图结束了他的巨著.

开普勒的玄秘说

思维玄秘的希腊人把正多面体和宇宙中的四行[②]配应起来.开普勒[③](J. Kepler)是这样论证这些配应的:这五种形体之中,正四面体的体积面积比最小,正二十面体的体积面积比最大;所以它们显示着干与湿的特性,因而配应于火与水.正立方体牢立于其底面上,与稳固的土地配应;正八面体可以绕任两对顶的连线为轴而旋转,配应于易流动的空气.正十二面体和宇宙相配应,因为黄道宫图数为12.他在正四面体上画一堆篝火,正二十面体上画一只虾和一条鱼,在正立方体上画一棵树、一根胡萝卜和园艺工具,在正八面体上画些鸟和云,并在正十二面体上画着太阳、月亮和星,以此表明上述配应.

对于这些多面体的每一个都可以作三个同心球面:一个(“外接球面”)过所有的顶点,一个和所有的棱相切,另一个(“内切球面”)和所有的面相切.考虑第二个球面.如果把每一条棱换
[133] 为垂直于此棱并与该球在同一点相切的直线,则汇于同一顶点的诸棱换为一个多边形.这些多边形正是另一个“反”多面体的 V 个面,此多面体有 F 个顶点.$\{p,q\}$的反多面体是$\{q,p\}$.所以,正立方体与正八面体互反.正四面体自反,即,与另一正四面体互反.一个正立方体的各个面上的对角线是两个互反正四面体的棱(参看图5.3中的第27图).“反”这个字的根据是存在着一个反演球,$\{q,p\}$的顶点正是$\{p,q\}$的面关于该球的极点,反

① T. Heath, A History of Greek Mathematics, oxford, 1921, Vol. I, p. 162.

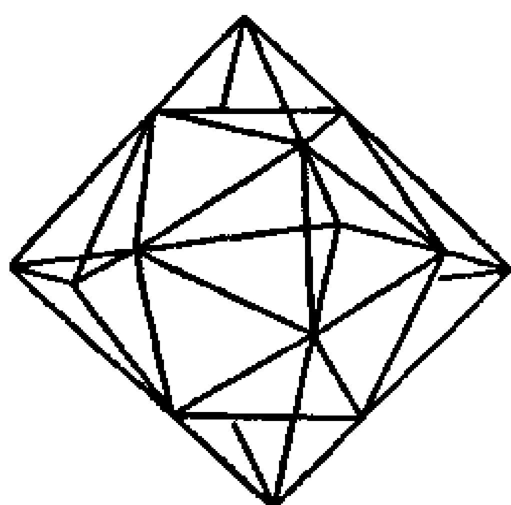
② 指“水、火、地、风”.——译者注

③ Opera Omnia, Frankfort, 1864, Vol. V, p. 121.

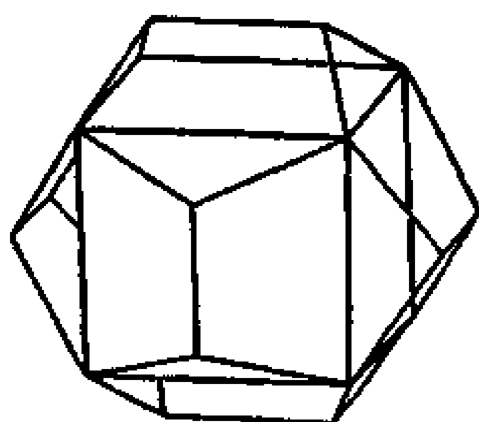
我们必须知道,而且我们必将知道

http://maths352.bokee.com

之亦然. 正立方体的外接球半径 R 与内切球半径 r 之比和正八面体的外接球半径与内切球半径之比相等，正十二面体的这个比值与正二十面体的这个比值也相等. 事实上，设反演球的半径为 ρ，则反多面体的外接球半径为 ρ^2/r，内切球半径为 ρ^2/R. 因此，要想使两个互反的正多面体有相同的外接球半径与相同的内切球半径，就必需适当调整它们的相对大小.（一般地说，它们的相当棱不再相交.）



正二十面体与正八面体



正立方体与正十二面体

图 5.2

帕普斯(Pappus)的顶点分布[1]

如果把两个具有相同内切球半径（当然也就有相同外接球半径）的两个互反正多面体并排放在一个平面（如桌面）上，则它们的顶点在各个水平面上的分布相同，即，层数相同且相当层上顶点个数之比也相同. 这是帕普斯[2]首先注意到的，虽然它的各种推广显示出这决非偶然，但直到晚近才得到恰当的解释. 此类推广之一是推广到开普勒－普安索（Kepler－Poinsot）多面体，后

① 此小标题为译者所加.

② T.Heath, A History of Greek Mathematics, Vol.Ⅱ, pp. 368—369.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

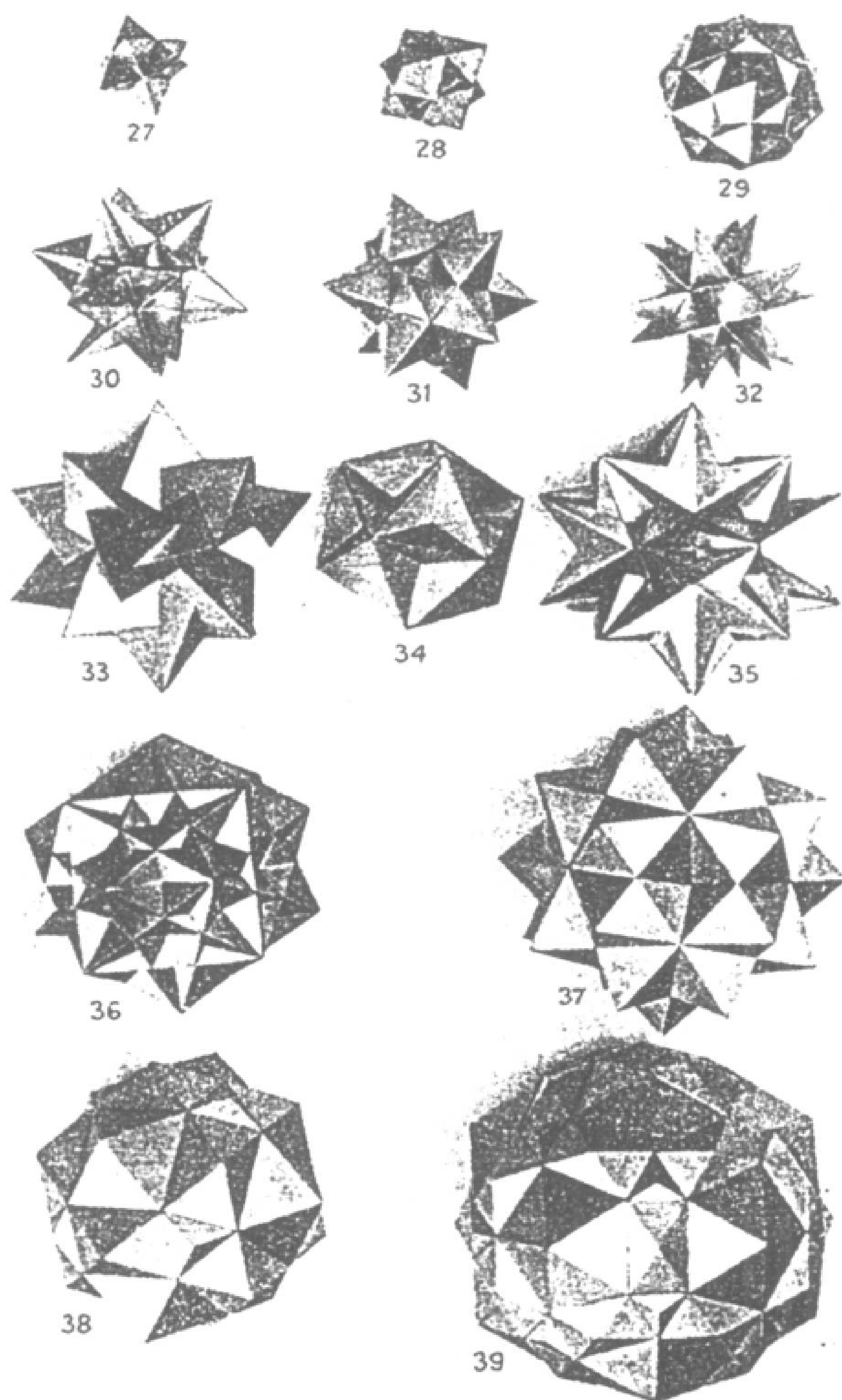


图 5.3

我们必须知道，而且我们必将知道

边即将谈到它. 另一种推广是推广到平面拼砌. 考虑拼砌{6,3}(即,围绕每个顶点有三个六边形). 从每个六边形里适当挑选相隔的顶点,则得到三角形拼砌{3,6}(由余下的顶点得出的是反拼砌). 于是我们可以看到,每个与{6,3}的一片同心的圆所包含的属于{6,3}的顶点和属于{3,6}的顶点一样多.(这是显然的,因为{6,3}的被弃去的顶点正是和原来的{3,6}全等的另一个{3,6}的顶点.) [134]

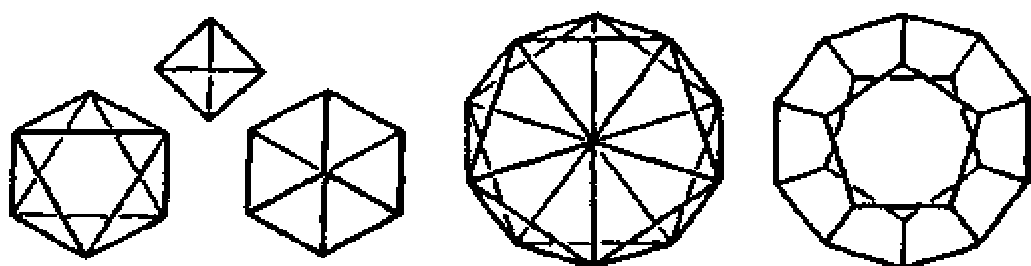
复合体

一个六角形拼砌的顶点同时也是两个三角形拼砌的顶点,这件事类似于上述事实——正立方体的顶点同时也是两个正四面体的顶点. 可以说这两个正四面体构成一个*复合体*——开普勒的*八芒星*(Stella octangula);它的八个面位于一个正八面体的表面所在的诸平面里. 还有由*五个正四面体*构成的复合体,其顶点是一个正十二面体的顶点而其面位于一个正二十面体表面所在的那些平面里;这样的正十二面体有一对. 把这一对正十二面体合到一起,使它们有共同的 20 个顶点,我们得到一个由*十个正四面体*构成的复合体,其中位置相反的每一对可代之以一正立方体,共用*五个正立方体*(与正十二面体有共同的 20 个顶点,每个顶点占用两次). 在一个给定的正十二面体里摹想一个这样的正立方体是很容易的(参看 139 页上的右图);这一组五个立方体组构成一个很漂亮的模型. 最后,将这五个正立方体进行反演,得到由*五个正八面体*构成的一个复合体,它的各个面位于一个正二十面体的各面所在的诸平面里,每个平面被占用两次. 这个正二十面体内接于每个正八面体内,见图 5.2 中的左图(参看图 5.3 中的第 27,33,35,36,37 诸图).

从一个正多边形的诸棱中,很容易挑出一些组成一条曲曲折折的多边形,其中第一条棱与第二条棱是某个面的两邻边,第二条棱与第三条棱又是另一个面的两邻边,等等. 这样的折线形称为*皮特里*(T.F.Petrie)*多边形*,它有很多应用. 每一个有限多

我们必须知道,而且我们必将知道

http://maths352.bokee.com



柏拉图体和它们的皮特里多边形

图 5.4

边形都可以正投影到一个平面上使一个皮特里多边形的投影是一个正多边形和可能有的被围在里边的另一部分. 可以用各种简单的方式证明一个皮特里多边形$\{p,q\}$有h条边，这里

$$\cos^2(\pi/h)=\cos^2(\pi/p)+\cos^2(\pi/q).$$

皮特里多边形$\{p,q\}$的h条边与反多面体$\{q,p\}$的h条棱相交；它们构成$\{q,p\}$的一个皮特里多边形.

正多面体有很多不同的对称性. 通过每个面的中心有一条
[135] 对称轴，通过每条棱的中点、通过每个顶点也都有一条对称轴：共有$E+1$条对称轴. 还有$3h/2$张对称平面.

阿基米德体

如果一个多面体的面都是正多边形并且存在着对称变换，它把一个指定的顶点依次变到其余的每个顶点，那么称此多面体为匀称的(uniform). 柏拉图体都是匀称的；高度适当(即当它们的侧面都是正方形、正三角形时)的正棱柱、反棱柱也都是匀称的. 此类多面体可用符号记之，符号给明围绕一个顶点的面的边数(按适当的轮换次序)；如n棱柱与反棱柱分别记为$4^2\cdot n$与$3^3\cdot n$. 容易证明①，除此两种之外还有下列 13 种(有限的、凸

① 参看 T. R. S. Walsh, Geometriae Dedicata, 1972, Vol. Ⅰ, pp. 117—123.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的)匀称多面体：

$$3\cdot6^2,\ 4\cdot6^2,\ 3\cdot8^2,\ 5\cdot6^2,\ 3\cdot10^2,\ 4\cdot6\cdot8,\ 4\cdot6\cdot10,$$
$$(3\cdot4)^2,\ (3\cdot5)^2,\ 3\cdot4^3,\ 3\cdot4\cdot5\cdot4,\ 3^4\cdot4,\ 3^4\cdot5.$$

这些多面体就是阿基米德(Archimedes)体.

令 σ 表示在一顶点处的表面角之和.(为了构成一个立体角,它必须不大于 2π.)于是,公式①$(2\pi-\sigma)V=4\pi$ 确定了顶点的个数.例如,$3^4\cdot5$ 有 60 个顶点,因为 $\sigma=\left(\frac{4}{3}+\frac{3}{5}\right)\pi$.

如果把八芒星看成是两个穿插起来的正四面体,那么可以说它们的公共部分是一个正八面体.而且,如已看到,它们的棱 [136]
是一个正立方体的面上的对角线.相仿地,当一个正立方体和一个正八面体处于互逆位置时(相应的棱彼此垂直平分),它们的公共部分是正立方八面体$(3\cdot4)^2$.每一对相应的棱(分别属于正立方体和正八面体)都是一个菱形的对角线,十二个这样的菱形构成一个"半正"(Semi-regular)多面体,称之为十二菱面体.(它不是匀称的而是"等面的".参看图 5.11 中的左图.)适当扩张之后,正立方八面体的棱与十二菱面体的棱相交成直角;事实上,这两个多面体是互反的.相仿地,正二十面体与正十二面体相穿插时,得出二十－十二面体$(3\cdot5)^2$,并导致它的反体三触面体(triacontahedron).(参看图 5.3 中的第 28,29 图与图 5.1 中的第 12,10,20,18 图.比较第 109 页上的拼砌.)5 个正立方体的复合体有三触面体的 30 个面,反之,5 个正八面体的复合体有二十－十二面体的 30 个面.

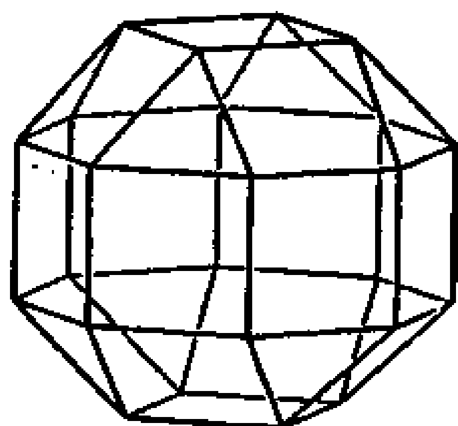
二十－十二面体的面由 20 个三角形和 12 个五边形(与两个亲原的正多面体相应).它的 60 条棱被其反三触面体的棱垂直平分(但后者的棱非被前者的棱平分.参看图 5.3 中的第 39 图.)这

① E. Steinitz and H. Rademacher, Vorlesungen über die Theorie der Polyeder, Berlin, 1934, p. 11.

我们必须知道，而且我们必将知道

[redacted]

些棱偶的60个交点是一个多面体的顶点，此多面体的面包括20个三角形、12个五边形和30个长方形．把这些点稍稍（向着三触面体的棱的中点）移动一下，这些长方形可变为正方形，从而获得另一个阿基米德体——二十－十二菱面体3·4·5·4.（见图5.1中的第23图；比较拼砌3·4·6·4.）一个类似的构造导致立方八菱面体$3\cdot 4^3$，它的面包括8个三角形和6＋12个正方形（见图5.3中的
[137] 第38图与图5.1中的第13图）．在试图制作这个多面的模型时，J·C·P·米勒[①]偶然地发现了一个“伪立方八菱面体”，它也是以8个三角形和18个正方形为面，并在不严格的即“局部的”意义上是等角的（每个顶点都由一个三角形和三个正方形围着），但不是在严格的意义上等角的（它要求当依次从每个顶点去观看这个立体时，其整体的外观都是一样的）．



伪立方八菱面体

图 5.5

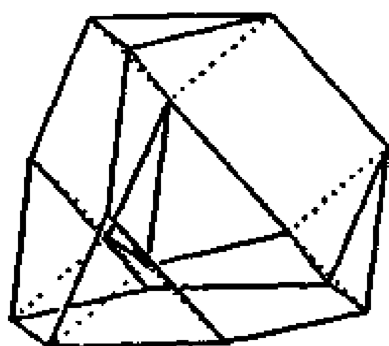
用平行于反八面体表面的平面去切掉一个正立方体的各个角尖，我们得出一些小三角形并且把原来的正方形面都变成了八边形．适当选取切割平面的位置时，这些八边形都是正八边形，并

① Philosophical Transactions of the Royal Society, 1930, series A, Vol, CCXXIX, p. 336.

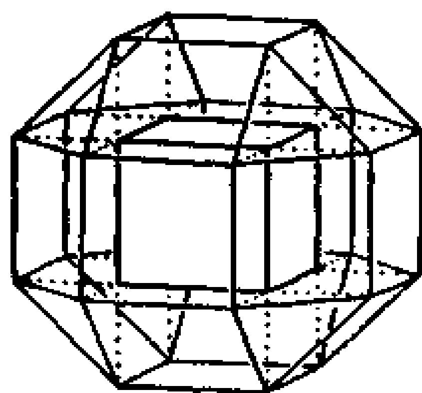
http://maths352.bokee.com



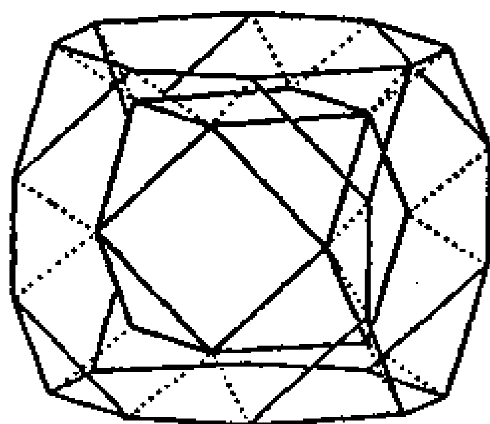
且得到另一个阿基米德体——截顶立方体，$3\cdot 8^2$(比较拼砌 $4\cdot 8^2$ 与 $3\cdot 12^2$)．5 个柏拉图体中每一个都有其截顶变体①；所以有立方八面体和二十－十二面体，不过在后两种情况里($4\cdot 6\cdot 8$ 与 $4\cdot 6\cdot 10$)又需要一次调整，将长方形变为正方形②(比较拼砌 $4\cdot 6\cdot 12$)．



(1) 正四面体与截顶正四面体



(2) 正立方体与立方八菱面体



(3) 截顶立方体与立方八面体

图 5.6

① “$\{p,q\}$的截角变体”是 $q\cdot(2p)^2$．见图 5.1 中的第 11,15,16,25,22 图．

② 由于这种变形，有时也把截了角的立方八面体($4\cdot 6\cdot 8$)叫做“大菱形立方八面体”，于是把 $3\cdot 4^3$ 叫做小菱形立方八面体．对于截了角的二十－十二面体和菱形二十－十二面体也有类似的叫法．

我们必须知道，而且我们必将知道

http://maths352.bokee.com



所有以上讨论过的阿基米德体都是自反射的(以任一棱的

[138] 中垂平面为镜面作反射).然而其余的两个都不是可反的,那就是狮鼻立方体 $3^4\cdot4$ 与狮鼻十二面体 $3^4\cdot5$(图 5.1 中的第 17 及 21 图).让我们在二十－十二菱面体的 30 个正方形的每个面上画一条对角线,这有两种可能,要那样去选择一种,使原 60 个顶点中每个顶点恰有一条选出的对角线通过它.(第一个正方形面上的选择决定了其余的一切.)此刻每一个正方形被剖分为两个等腰直角三角形.作形变使它们都变成等边三角形,我们就得到狮鼻十二面体①.相仿地可以从菱形立方八面体导出狮鼻立方体,只要记住,我们只对于和正立方体的棱相应的 12 个正方形(而不对于和它的六个面相应的正方形)开刀.拼砌 $3^4\cdot6$ 可以看成是一个"狮鼻体{6,3}",而 $3^2\cdot4\cdot3\cdot4$ 可以看成是一个"狮鼻体{4,4}".此外,"狮鼻四面体"就是正二十面体{3,5},可由正立方八面体(或"四四菱面体")仿上导出.

狮鼻正立方体和狮鼻正十二面体二者出现在一对变体里.它们的尺度需解一个三次方程,而自反射的阿基米德体(以及正多面体)的尺度只需要求平方根;换句话说,可反体是可用欧几里得构图法作出的,但这两个真正的狮鼻体则不能.

斯托特夫人作图法

上边对阿基米德体的描述基本上是开普勒的.艾丽西亚·布尔·斯托特(Alicia Boole Stott)②曾设计出了可反射形体的一种漂亮得多的构图法.她的方法用不着任何形变,而且最终的棱长与开始时的正多面体的棱长一样.在称为外膨的过程中,

① 这个名称不大好,因为这个形体与二十面体的关系和它与十二面体的关系一样密切.称之为"狮鼻二十－十二面体"也许更好一些.

② Verhandelingen der Koninklijke Akademie van Wetenschappen, Amsterdam, 1910, Vol. XI, no. 1.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

某些元(即,棱或面)的集合沿着离开中心的方向直接移开,同时保持它们原来的大小和方位,直到所产生的缝隙可以装进 [139]
新的正多边形面.相反的过程称为内收.外膨任一正多面体的所有的棱,就导出"截角"变体.外膨正立方体的(或正八面体的)所有的面,就导出菱形立方八面体,$3\cdot 4^3$.再外膨其与正立方体的棱相应的12个正方形,或者外膨截角正方体的八边形面,就导出截角正立方八面体,$4\cdot 6\cdot 8$.内收截角正立方体的所有三角形面,导出正立方八面体.如此等等.斯托特夫人曾用一套紧凑的符号表示这些过程,并把它们推广应用于高于三维的空间里,其收获异常丰富. [140]

等边环带多面体

下边我要描述的一些体是首先被费多罗夫(E.S.Federov)①研究过的体.由于唐奇安(P.S. Donchian)的洞察而使其趣味大大增加了.他看出这些立体可以被看成是 n 维超立方体(或测度多胞形及棱正交的正则多胞形②)的三维投影.它们的棱都相等,它们的面一般地是菱形,但有时是高级"平行边 $2m$ 角形,"即,中心对称的等边 $2m$ 角形.论题从下列关于多边形剖分的定理开始.

每个平行边 $2m$ 角形(特别是,每个正 $2m$ 角形)都可以剖

---

① Zeitschrift für Krystallographie und Mineralogie, 1893, Vol. XXI, p. 689; Nachala Ucheniya o Figurakh, Lenigrad, 1953. 又见 Coxeter, Twelve Geometric Essays, Carbondale, Illinois, 1968, chap. 4.

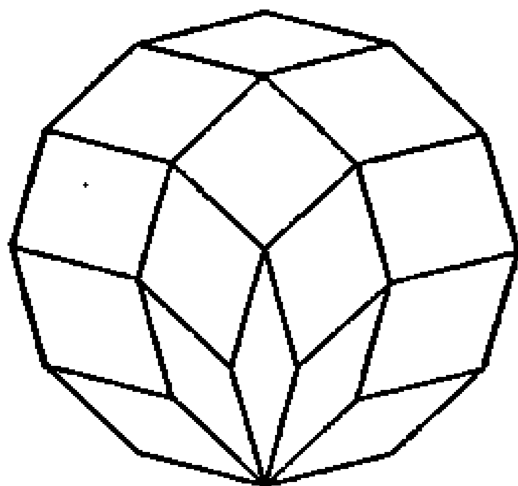
② L.Schläfli, Quaterly Journal of Mathematics, 1860, Vol. Ⅲ, p.66: "(4, 3, 3, ⋯, 3)"; C. H. Hinton, The Fourth Dimension, London, 1906; P.H. Schoute, Mehrdimensionale Geometrie, Leipzig, 1905, Vol. Ⅱ, pp. 243—246; D. M. Y. Sommerville, An Introduction to the Geometry of n Dimensions, London, 1929, pp. 49, 171, 182, 190.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

分① 成$\frac{1}{2}m(m-1)$个边长相等的菱形.不难用归纳法证明这个论断,因为每个平行边$2(m+1)$角形可看成用一条m个菱形接成的"带子"加添到一个平行边$2m$角形上而构成.事实上,这个$2m$角形的平行边偶可以取任何m个不同的方向,而相应于这些方向的每一对边都有属于上述带中的一个菱形;故其数目为$\frac{1}{2}m(m-1)$.和两个相互垂直方向相应的菱形是正方形.

现在考虑取通过空间一点的任一n条线束②,并先假定这些直线中的任何三条都不共面.于是有这样一个多面体,它的表面是由$n(n-1)$个菱形组成的,并且它的棱分为n组,每组包含相互平行的$2(n-1)$条,分别平行于所取的n条直线.事实上,对应于这n条直线中的每一双都有一双相向的面,其边平行于这一双直线.为了构造这个等边环带多面体,想象把通过这n条直线中任一条的一张平面慢慢转一整圈.每当这个平面经
[141] 过其余$n-1$条直线中的某一条时,就作一个两邻边分别和这



在一个十二角形里的十五个菱形

图 5.7

① 有多少个方式?

② 这个构图法属于唐奇安.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

两条直线平行的一个菱形，并且把它毗连到(不要变动它的方位)先前的一个菱形上.这个过程最终导出一个由 $2(n-1)$ 个菱形连成的封闭的带子.再把我们的注意力转到这 n 条直线的另一条上，依法构造，又得到另一条带子，它有两个相互平行的面，这两个面是与第一条带子公有的.当造完了可能有的一切带子之后，多面体也就完成了.

如果这 n 条线之中有 m 条共面，则代替相向的 $\frac{1}{2}m(m-1)$ 对菱形的是一对相向的平行边 $2m$ 角形.如果这 m 条线的布置是对称的，则此 $2m$ 角形将是正 $2m$ 角形.

特别是，三条相互垂直的等长线段导出一个正立方体，三条非相垂直的等长线段导出一个菱面体①(或斜方棱柱).一般地，m 条共面线段和另一条线段导出一个平行边 $2m$ 棱柱(当这“另一条”线垂直于前 m 条线所在的平面时，得到的是一个正棱柱).

正立方体的 4 条“直径”(两对顶的连线)导出十二菱面体，正二十面体的 6 条直径导出三触面体，正十二面(五角形面)体的 10 条直径导出一个九触面体②，它的面是 30 个相同的菱形 [142]
和 60 个另一种菱形.正立方八面体的 6 条直径导出截角八面体，它的面是 6 个正方形和 8 个六角形(等价于 8×3 个菱形)，二十-十二面体的 15 条直径导出截角二十-十二面体，它的面是 30 个正方形，20 个六角形($=20\times3$ 个菱形)和 12 个十边形($=12\times10$ 个菱形).作为最后一个例子，正八面体和正立方八面体(适当地放在一起)的 9 条直径③导出截角正立方八面体，它的面是 12 个正方形，8 个六角形($=24$ 个菱形)和 6 个八角形($=36$ 个菱形)(参看图 5.1 中的第 10,18,24,16,26,19 图).

---

① 使用这个名称时，我并不是说这六个菱形面都相同.

② 它有些像夏普(A. Sharp)著 Geometry Improv'd，第 87 页上的一个图.

③ 即，正立方体(或正八面体)的 9 个对称平面的垂线.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

在这些例子里，多面体和所给的直线束有同类型的对称性，一般情况下也是如此.一束对称地布置在一个圆锥周围的任意 n 条直线导出具有对称中心和一组 n 个对称轴的斜方 $n(n-1)$ 面体①.当 $n=3$ 时，所有的面都相同；当 n 为 4 或 5 时，如果这些直线选择得适当(即若相邻直线的夹角与相隔直线的夹角互补)时，所有的面也都相同.当 $n=4$ 时导出十二菱面体；当 $n=5$ 时导出二十菱面体②(图 5.1 中的第 14 图)，它可以由三触体经过去掉任何一个环带并把剩下的两部分拼合到一起而得到.从二十菱面体适当地去掉一个环带，就得到比林斯基(S. Bilinski)的新十二菱面体，它的面统统一样，但与古典的十二菱面体不同.

将等边环带多面体的沿某方向的棱都伸长或都缩短，就得
[143] 到费多罗夫的一般环带多面体.这样一来，那些菱形面都变成了平行四边形，而"平行边 $2m$ 角形"不再是等边的了.当所有高级的面都换为同样多的平行四边形后，我们得到 $F=n(n-1)$，$E=2F$，且 $V=F+2$.事实上，每个完全以平行四边形为面的凸多面体都是等边环带多面体③.

关于这个论题的一个最后的注记：前边证明过的定理——平行边 $2m$ 角形可以剖分为 $\frac{1}{2}m(m-1)$ 个平行四边形——有一个三维的类推，即，环带多面体可以剖分为 $\frac{1}{6}n(n-1)(n-2)$ 个平行六面体(即，n 个方向中每三个的组合对应着一个).

开普勒－普安索多面体

延伸正五边形的各边直到它们再次相交，得到所谓五芒星

① B.L. Chilton and H.S.M. Coxter, American Mathematical Monthly, 1963, Vol. LXX, pp.946—951.

② Stanko Bilinski, Glasnik, 1960, Vol. XV, pp.252—262.

③ Coxter, Regular Polytopes, New York, 1963, p.27.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

形，长久以来它都被用为一个神秘的符号.我们可以把五芒星$\left\{\frac{5}{2}\right\}$看成一个广义的多边形，它有五条边，而这五条边接连地画出时恰围绕其中心两周.每条边在中心张成一个角度为$\frac{4}{5}\pi$的角，而一个普通正 n 边形的每条边在中心张成的角度是$2\pi/n$.因此一个五芒星形就好像是一个边数为 $n=\frac{5}{2}$的 n 边形.相仿地，任一个有理数 $n(>2)$都对应着一个$\{n\}$边形，n 的分子表示边数，分母表示“密度”(或“品类”).

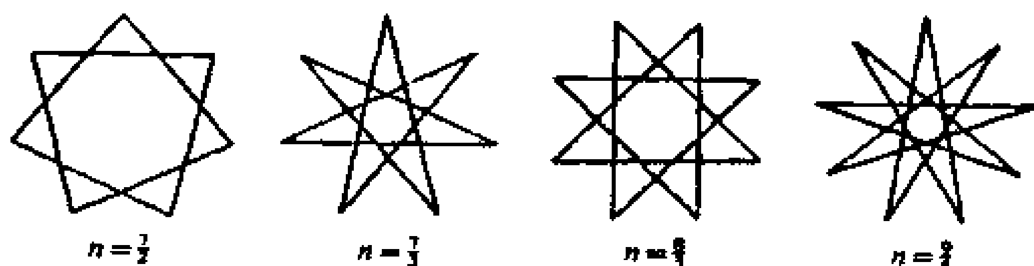


图 5.8

这个“成星”步骤也可用于空间的图形.正十二面体的成星面以 5 个面汇交于一点，共得 12 个新点(星尖)，形成小星形十二面体$\left\{\frac{5}{2},5\right\}$.这些新点也属于一个二十面体.将这个二 [144]
十面体的棱画出来并保留原来的 12 个面，我们得到一个多面体，它的面是 12 个通常的五角形，但其在顶点附近的截面都是五芒星；这就是大十二面体①，$\left\{5,\frac{5}{2}\right\}$.这符号已表明它与$\left\{\frac{5}{2},5\right\}$是互反的.将$\left\{5,\frac{5}{2}\right\}$的面星化，就得到大星形十二面

① 不列颠百科全书(Encyclopaedia Britannica)第 14 版，“Solids”条目下不适当地将它称为“小星形十二面体”并把小的称为大的.(比较第 11 版，“Polyhedron”条目.)

我们必须知道，而且我们必将知道

http://maths352.bokee.com

体$\left\{\frac{5}{2},3\right\}$，其星尖是一个普通十二面体的二十个顶点．它的反体，大二十面体①$\left\{3,\frac{5}{2}\right\}$有二十个三角形面，它的星尖是一个普通二十面体的顶点(参看图 5.3 中第 31，34，32，30 图)．

于是我们把正有限多面体的个数从 5 增加到 9．可能的情况也只有这 9 种②．这个论断可以证明如下：注意即使 p 与 q 不是整数，“皮特里多边形”$\{p,q\}$仍然由数字 h 标志着，其中

$$\cos^2(\pi/h)=\cos^2(\pi/p)+\cos^2(\pi/q).$$

将这个方程改写成对称形状：

$$\cos^2(\pi/p)+\cos^2(\pi/q)+\cos^2(\pi/k)=1,$$

其中 $1/k=1/2-1/h$．我们发现它的有理解是 3，3，4 的 3 种排列和 3，5，$\frac{5}{2}$的 6 种排列，总共 9 种．

$\{p,q\}$	V	E	F	D	名　　称	发现者
$\left\{\frac{5}{2},5\right\}$	12	30	12	3	小星形十二面体	开普勒(1619)
$\left\{\frac{5}{2},3\right\}$	20	30	12	7	大星形十二面体	(同上)
$\left\{5,\frac{5}{2}\right\}$	12	30	12	3	大十二面体	普安索(1809)
$\left\{3,\frac{5}{2}\right\}$	12	30	20	7	大二十面体	(同上)

[145]

① 吕卡斯在他的 Récréations mathématiques (Vol. Ⅱ, pp.206—208, 224)里给出了这些形体的精美绘形．

② 柯西(A. L. Cauchy)首先(用别的方法)证明了这个论断．见于 Journal de l'Ecole Polytechnique, 1813, Vol. Ⅸ, pp.68—86.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

通常的多面体都适合欧拉公式 $V-E+F=2$，但多面体 $\left\{\frac{5}{2},5\right\}$ 与 $\left\{5,\frac{5}{2}\right\}$ 都不适合它（显然，这个事实使得施勒夫利(L. Schläfli)[①]否认这两个多面体的存在），本书第 8 章里将说明其原因．然而，所有这 9 种正有限多面体都适合凯莱(A. Cayley)的下列推广的公式：

$$d_V V - E + d_F F = 2D,$$

其中 d_F 是一个面的“密度”（即，对于一个通常的多边形为 1，对于一个五芒星为 2），d_V 是一个顶点（更确切地说是一个顶点附近的截口）的密度，D 是整个多面体的密度（即，面包围中心的层数）．

“阿基米德”星状体也已经被研究过[②]，但是超出了本书的范围．

59 种正二十面体

设想在一大块木头内部画上一个小的正四面体或正立方体．如果沿着这小立体的面所在的平面把木头锯开并把延伸到大木块表面的木头块拿开，那么剩下的除了四面体或立方体外就没有任何东西了．但是如果不是为了锯出一个正四面体或正立方体而是要锯出一个正八面体，那么锯成的将有 9 块：正八面体自身和每个面上的一个正四面体．它们在一起构成一个八芒星，其外貌是两个相互穿透的正四面体（上述正复合体）．相仿地，若要锯出一个正十二面体，则得到 1＋12＋30＋20 块：正十二面体自身，12 个五棱锥，30 个楔状四面体，和 20 个三角双锥．

---

① Quaterly Journal of Mathematics, 1860, Vol. Ⅲ, pp. 66, 67. 他阐明了“$\left\{\frac{5}{2},3\right\}$ 和 $\left\{3,\frac{5}{2}\right\}$”但未阐明“$\left\{\frac{5}{2},5\right\}$ 和 $\left\{5,\frac{5}{2}\right\}$”．

② Coxter, Longuet-Higgins, and Miller, Philosophical Transactions of the Royal Society, 1954, series A, Vol. CCXLVI, pp. 410—450.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[146] 它们合在一起构成大星形十二面体.

最后指出,按上述过程,正二十面体①导致 1 + 20 + 30 + 60 + 20 + 60 + 120 + 12 + 30 + 60 + 60 块,它们可以拼合成 32 种不同的立体,这些立体都有和正二十面体完全相同的对称性,另外还有 27 对立体,它们只具有旋转对称性.前一组立体包括原先要锯出的正二十面体、5 个八面体的组合(由前 1 + 20 + 30 块组成)、十个四面体的组合(由前 1 + 20 + 30 + 60 + 20 + 60 + 120 块组成)以及大二十面体(由除了最后 60 块之外所有的块组成).后一组包括五个四面体的组合和一些更复杂的形体,它们都具有同样优美的"扭挠的"外观②.

立 体 拼 砌

正如用正多边形铺满一个平面可以有许多对称的方式一样,也有许多对称的方式用正多面体和阿基米德多面体砌满空间.为简明起见,让我们的讨论限于那些方式,其中所有的棱(以及所有的顶点)都以同样方式被围绕着.这样的"立体拼砌"恰有 5 种③,围绕每个棱有(i)4 个正立方体,或(ii)相互交错的 2 个正四面体和 2 个正八面体,或(iii)1 个正四面体和 3 个截四面体,或(iv)3 个截八面体,或(v)1 个正八面体和 2 个正立方八面体.让我们用符号$[4^4]$,$[3^4]$,$[3^2\cdot6^2]$,$[4\cdot6^2]$,$[3^2\cdot4]$表示它

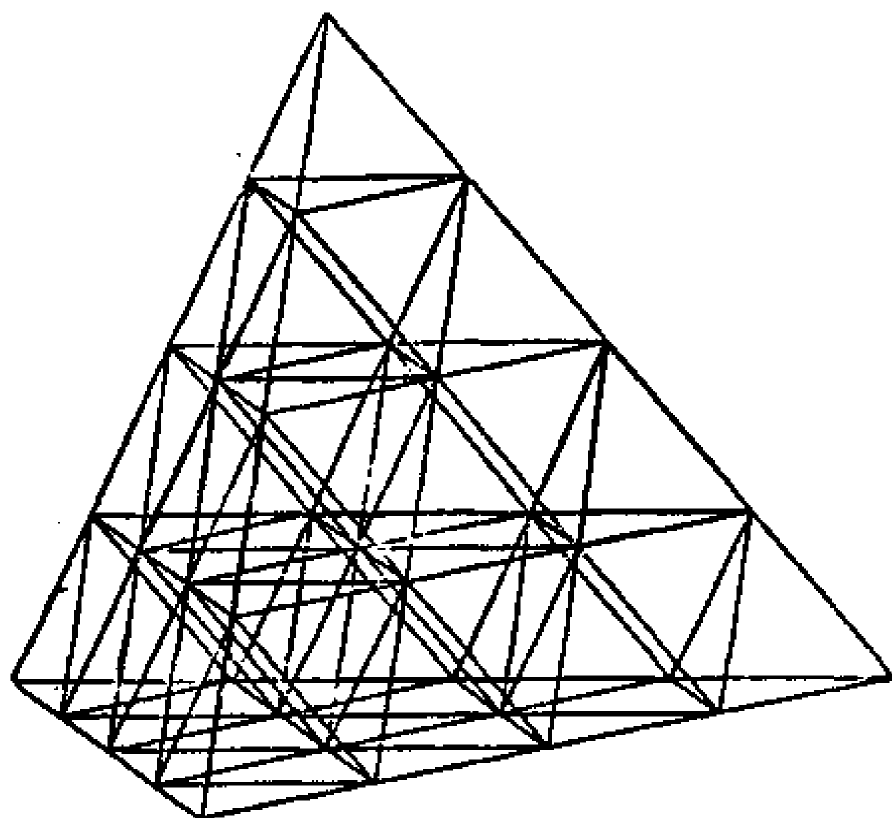
① A. H. Wheeler, Proceedings of International Congress, Toronto, 1924, Vol. 1, pp.701—708; M. Brücker, Vielecke und Vielfache, Leipzig, 1900(图片Ⅷ,第 2,26 图;图片Ⅸ,第 3,6,11,17,20 图;图片Ⅹ,第 3 图,图片Ⅺ,第 14,24 图).

② 要看皮特里(J.F. Petrie)绘制的这些精美的图形,参看"The 59 Icosahedra", University of Toronto Studies (Mathematical Series), no. 6, 1938.

③ A. Andreini, Memorie della Società italiana delle Scienze, 1905, series 2, Vol. XIV, pp.75—129,第 12,15,14,18,33 图.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



立体拼砌 $[3^4]$

图 5.9

们.这些数字表明汇于一个棱的界面正多边形.

"正则"空间拼砌 $[4^4]$ 是人人熟悉的.所有正立方体的中心恰好是一个同样的空间拼砌的所有的顶点.在这个意义上,正则空间拼砌是"自反的".它的交错的顶点给出空间拼砌 $[3^4]$, [147] 每个正立方体里内接着一个正四面体,并且包围着每个其余的顶点有一个正八面体.这个拼砌有特殊高度的正规性(虽然它用了两种立体块,不像 $[4^4]$ 那样仅用一种),因为不仅顶点和棱,而且所有的三角形分界面所邻接的子块也是相同的;事实上,每个三角形的一侧是正四面体而另一侧是正八面体.如果把相邻子块的中心用垂直于分界面的连线和垂直于棱的平面连接起来,我们就得到"反"拼砌,不妨记为 $[3^4]'$;这种拼砌由十二菱面体组成,其中 4 个围绕一些顶点(原拼砌的正四面体块

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的中心),其余 6 个围绕另外一些顶点(原拼砌的正八面体块的中心).

空间拼砌[$3^2\cdot 6^2$]可从[3^4]导出,为此只须将后者的一定的正四面体集合中的每一个都与其相邻的 4 个正八面体以及另外
[148] 6 个正四面体黏合为一体,这些四面体把它们成对地黏合而形成一个截四面体①.于是[$3^2\cdot 6^2$]仅有[3^4]的顶点的半数,而[3^4]又仅有[4^4]的顶点的半数.

截八面体的空间拼砌[$4\cdot 6^2$]是"等腰"四面体(或正方双楔体)拼砌的反拼砌,后者的顶点属于两个反[4^4](晶体学中的"体心立方格子").[$3^2\cdot 4$]的顶点是[4^4]的棱的中点(或正方形面的中点).

摞球或密装

将一些同样大的小球一层摞一层地装满一个大盒子,有多种不同的装法,我要述说其中的三种.可以这样装:每个球置于下一层的 1 个球正上方并与同一层的 4 个球和上一层的 1 个球相接触;所以每个球与另 6 个球相接触②.另一装法是把每层的球稍稍散开一些,使它们不再相接触而让每个球架在下一层的 4 个球上并且参与支持上一层的 4 个球.要调整这一"散开"使这 8 个接触点成为 1 个正立方体的 8 个顶点.还有一种用球装满盒子的装法,那就是使每个球既与下一层的 4 个球相接触,又与同一层的 4 个球相接触,而且还与上一层的 4 个球相接触.最后这种安排就是所谓规范垒装(Normal piling)或球体密装(Spherical close-packing),它给出了一定的盒子内可能装填半径

---

① 相仿地,平面拼砌 6^3,$(3\cdot 6)^2$,$3^4\cdot 6$ 的任一种都可以从 3^6 导出,为此只须将一些 6 个三角形的集合并成一些六角形.

② 底层、顶层、四周的球当然除外,且球的半径是盒底的长度与宽度的公因数.下同.——译者注

我们必须知道,而且我们必将知道

http://maths352.bokee.com

一定的小球的最大数目.(虽然一个球不可能同时接触 12 个以上与自身一样大的球,我们将在下边看出却有许多不同的装法使每个球同时接触 12 个与自身一样大的球.)

这三种装法可再描述如下:在第一种装法里,各个球心是空间拼砌[4^4]的顶点,各个球自身分别内切于反拼砌[4^4]的 [149]
各个正立方胞腔.在第二种装法里,那些球内切于[$4\cdot6^2$]的截八面体(接触各个正六边形,但不接触各个正方形).在第三种装法里,那些球内切于[3^4]′的十二菱面体,而球心是[3^4]的顶点.

空间拼砌[3^4]的顶点形成一系列平行平面上的三角形拼砌 3^6.

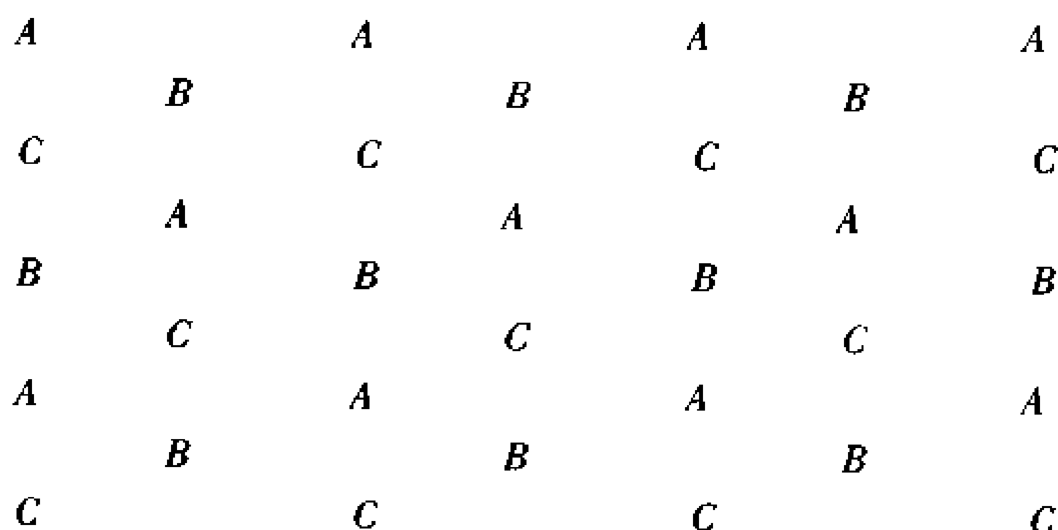
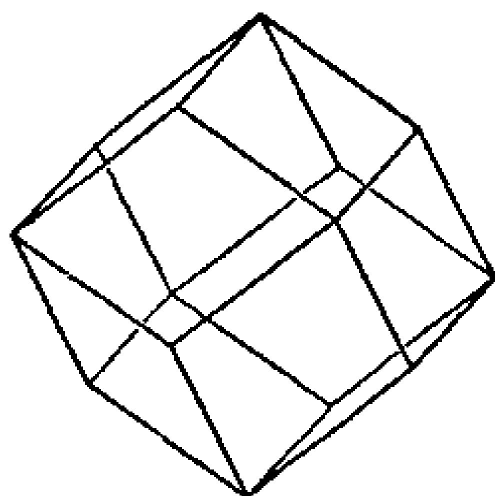


图 5.10

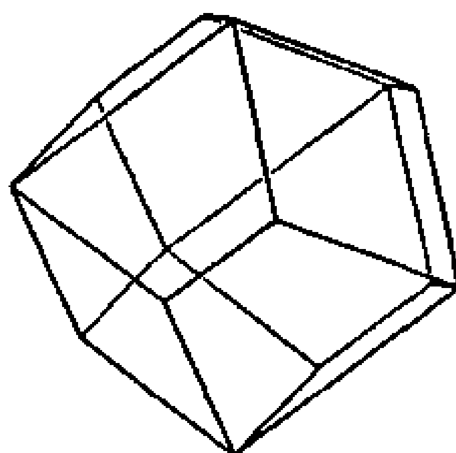
上图表明这种装法的球心点阵在一个水平面上的正投影.点 A 是从一个平面投影来的,点 B 是从下一个平面投影来的,点 C 是从再下一个平面投影来的,然后又从更下一个平面投影来 A,如此循环下去.现在设想把球体的中心都放在这些点上.所有的 A 点给出一层密集的球,每一个和周围的六个球相切.点 B 的集表示另一这样的层,它们架在第一层上.点 C 的集表示第三个这样的层,架在第二层上.但是如果第三层的各个球心不处于诸 C 点的上方而处于诸 A 点的上方,那么这个装法是和

我们必须知道，而且我们必将知道

http://maths352.bokee.com



（1）斜方十二面体



（2）梯形斜方十二面体

图 5.11

上述装法是同等“经济”的．所以，在装添任何一层时，新的一层可以摆在倒数第二层的正上方，也可以不摆在倒数第二层的正
[150] 上方．

排列 *ABCABC*…表示球的密装法；另一方面，排列 *ABABAB*…称为*六角形密装法*．在这两种情况下，空间被填充的程度都达到了 74%．如果把许多同样大的“橡皮泥”或做模型用的黏土制成的小球先在粉笔灰里滚一滚，然后用任一种方式装起来再紧压成一块，然后松开来看时就会发现那些靠近中部的小球分别变成近似于十二菱面体和梯形斜方十二面体①．如果不去细心地垒装那些球而把盒子多晃动几次，使它们随机垒装自动达到最大可能的密度，然后像前边说的一样紧压成一块，松开看时就可以看到各种各样的不规则的多面体．它们的平均面数②不是 12 而接近于 13.3．这样随机填装的结果未见得比规范垒装占有的空间较少；但明显的是任何微小的移动都会扩大间隙而使总

① 参看 Steinhaus, Mathematical Snapshots, New York, 1938, p.88.

② J. D. Bernal, Nature, 1959, Vol. CLXXXIII, pp.141—147; Coxter, Introduction to Geometry, pp.410—412.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的体积增加.

海边的沙滩

如果你站在海边的湿沙滩上，很容易看到你的脚周围的沙子变得相对地干一些，而你留下的脚印里却渗出一汪水.下边的解释我相信是奥斯本·雷诺(Osborne Reynolds)给出的.沙粒受海浪的长期冲动而滚磨得近似于球形，它们的沉积过程大体上 [151]
是随机垒装.你的脚的踏压破坏了这种垒装，因而扩大了沙粒的间隙.周围的水就被吸过来去填充这些间隙.当你抬起脚时，随机垒装又部分地恢复了，所以有点水被留在上面.

正 海 绵 胞

前边第135页上关于"正则性"的定义的核心是两种对称变换.在迄今的讨论中，这些对称变换都是*旋转*.如果允许顶点数、棱数和面数都可以是无限大，那么这个定义就包括了平面拼砌{3,6}，{6,3}和{4,4}.允许每个面有无限多边或者允许围绕一个顶点有无限多个面是荒谬的，所以这种特殊的对称必须是周期的.然而，它们不必一定是旋转；它们可以是旋转反射.(一个*旋转反射*就是旋转与反射的组合.我们恒可取旋转轴垂直于反射面.)这种变换将多面体的"内部"与"外部"互换，因而内部与外部是恒等的，而且多面体(它把空间分为两个相等的部分)必定是无限大的.一个给定的面的棱处的二面角是正负交错的；汇于一个顶点的棱交错地处于某一平面的两侧.这样就允许有共同顶点的面－角之和超过 2π.

可以证明方程

$$2\sin(\pi/p)\sin(\pi/q)=\cos(\pi/k)$$

的正整数解组给出此类多面体$\{p,q\}$，那就是$\{6,6\}(k=3)$，$\{6,4\}$与$\{4,6\}(k=4)$，$\{3,6\}$与$\{6,3\}(k=6)$和$\{4,4\}(k=\infty)$.三种平面拼砌的发生是因为一个平面上的旋转完全可以看成是空间里的一个旋转或一个旋转反射.新的三种图形就是具

我们必须知道，而且我们必将知道

[redacted]

[152] 有 k 角形洞的"海绵胞".①

海绵胞{6,6}的面是空间拼砌[$3^2\cdot6^2$]的那些正六边形；{6,4}的面是[$4\cdot6^2$]的那些正六边形；{4,6}的面是[4^4]的正方形的半数.与这些空间拼砌的其他界面相应的是海绵胞上的空洞.后两种海绵胞(皮特里发现于1926年)是互反的，就是说一种的顶点是另一种的面心②；{6,6}是自反的，或者说，和另一个全等的{6,6}互反.

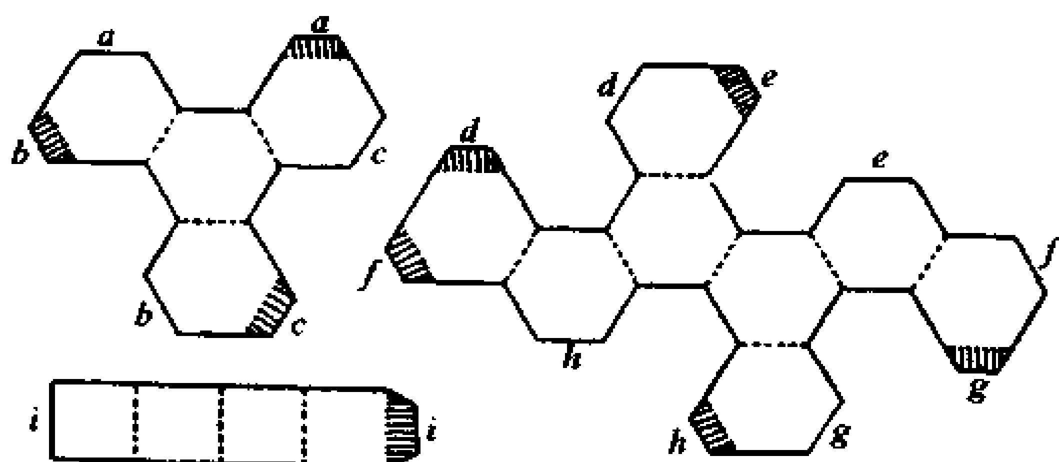


图 5.12

要制作海绵胞{6,6}的模型，可用薄卡片剪出4个相连的正六边形(参看图5.12)，然后把它沿虚线折转而黏合成一个截顶正四面体($3\cdot6^2$)，不过它的4个正三角形面都是空洞，然后再把许多相同的这种空胞黏到一起，使六边形面与六边形面相贴合.注意要使任一条棱只属于两个面.(在制成的模型里，面都是双层的.这使得不但容易制作而且较坚固.)相仿地，要制作海绵

① Coxter的Twelve Geometric Essays 77页上有这些模型的照片，那里把这三种海绵胞记为{6,6|3}，{6,4|4}，{4,6|4}.

② 平面拼砌也可以在这种意义上互反，但是有限多面体不行.正八面体的面心是一个正立方体的顶点，但是这个正八面体的顶点却是另一个较大的正立方体的面心.

http://maths352.bokee.com

胞{6,4}的模型,可先剪出(见图 5.12)八个相连的正六边形.它们是截顶正八面体($4\cdot6^2$)的六边形面.最后再说海绵胞{4,6}的制作是用一串相连的 4 个正方形.不过,最后这种模型是不稳固的.它可以逐渐垮下去,方洞变成菱形洞.(米勒有一次制作了一个大模型并把它压平、装到信封里寄了出去.) [153]

四面体的旋转环

安德列斯和斯托克(R. M. Stalker)各自发现了一族具有 $2n$ 个顶点,$6n$ 条棱(其中 $2n$ 条两两叠合)与 $4n$ 个三角形面的非稳固有限多面体,$n=6,8$ 或任何更大的正整数.它的面是 n 个四面体的面.这些四面体的每一个有两条相对的棱,其中之一与前一个四面体公用,另一条与后一个四面体公用,从而构成一种环状体.当 $n=6$ 时,活动的范围是相当小的,但当 $n=8$ 时,这个环就可以像烟圈似的不断翻转.当 n 为偶数时,这环有一个对称的稳定姿势;特别美观的是当 $n=10$ 时的样子①.当 n 为奇数时,由于完全没有对称性而使得活动起来的时候更美妙得多.当 $n\geqslant22$ 时,这个环可以呈纽结的形状.

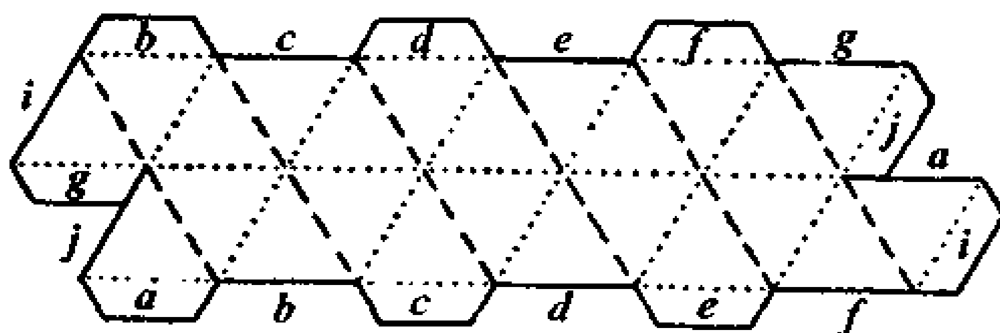


图 5.13

① 布吕克纳(M. Brückner)在他的 Vielecke und Vielflache 第 216 页上(以及图片Ⅷ第 4 图)所描绘的“王冠形”之一就是由十个非正的四面体组成的环.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



此类环中的任一个的模型都可以用一片纸制作出来.当 $n=6$ 时,仿绘上图,把它剪下来,再沿内部的虚线和点线分别向上和向下折起来,最后再把所有的小翅按字母所示贴到邻面上去.当 n 为 4 的倍数时,两端的连法稍异于此(参看第 221 页上的图 7.35).当 n 为奇数时,随便用哪一种连法都可以.

由于有两种类型的棱,这类多面体不算是正的.将等边三角
[154] 形都换为等腰三角形时,对称性不变.如果所有的二重棱都较别的棱短得多,即使当 $n=6$ 时[①]这个环也可以像 $n\geqslant 8$ 时一样随意翻转.

万　花　筒[②]

通常的万花筒是由两个夹角为 $\pi/3$ 或 $\pi/4$ 的平面镜和一个(或一组)小东西组成的,这个东西被置放在夹角内使得两个镜子里都反射它并相互反射.结果看到这物体有 6 个或 8 个像(视夹角大小而定),排列在优美的对称位置上.用合叶将两个(无框)镜子连到一起,于是两片镜子的夹角可以随意变动.很明显地可以看到当夹角为 π/n 时有 $2n$ 个像(包括物体本身).两镜子平行时是一种极限情况,这时理论上有无限多个像(实际上要受光照亮度与镜面质量的限制).如果物体是夹角平分面上的一个点,那么它的像就是一个正 $2n$ 边形的诸顶点.如果物体是镜子之一上的一个点,则像点两两重合于一个正 n 边形的诸顶

---

① 这样的环(有 6 个四角形的双楔)在美国曾经作为儿童玩具在市场上出售,在它的 24 个面上标着字母(1935 年特许专利第 1997022 号).参看 M. Goldberg, Journal of Mathematics and Physics, 1947, Vol. XXVI, pp.10—21.

② E. Hess, Neues Jahrbuch für Mineralogie, Geolcgie und Palaeontologie, 1889, Vol. Ⅰ, pp.54—65.

我们必须知道，而且我们必将知道

点上.这个点在实践中可用一支蜡烛的火焰或一个小塑料球或一点油泥子去表示它.

设想这两个镜子是竖直立着的.让我们再竖立起第三个镜子,使这三个镜子中两两的夹角都是 π 的几分之一.换句话说,三个镜子的任一水平截口三角形的三个内角分别为 $\pi/l,\pi/m,\pi/n$,这里 l,m,n 都是正整数.于是 l,m,n 应适合方程

$$\frac{1}{l}+\frac{1}{m}+\frac{1}{n}=1,$$

而它的解是 3,3,3; 2,3,6; 2,4,4. 在每种情况下,像都有无限多.改变物点在三角形内的位置,我们就得到某些等角拼砌的诸顶点①.特别当物点取在三角形的一个顶点上,或一个角的平分线与对边的交点上,或在内心(三条角的平分线的交点)上时,拼砌的马赛克都是正多边形.用第 109 页的记号可将各种情况下的结果示于下图中: [155]

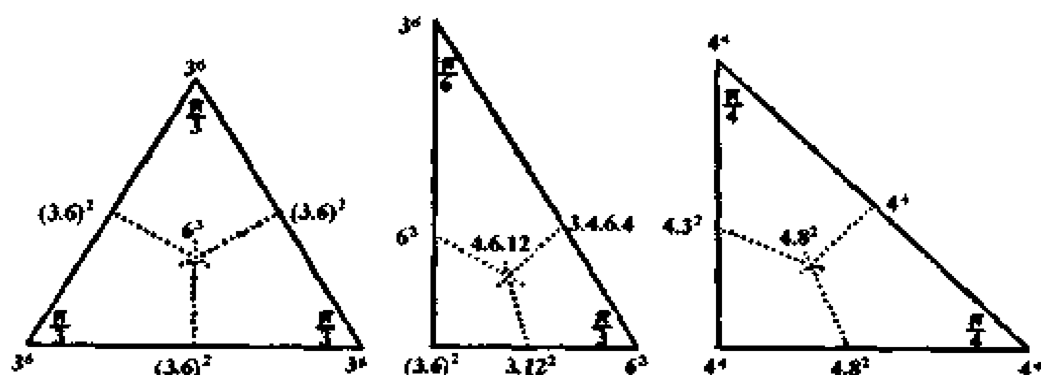


图 5.14

可以把镜子里出现的那种三角形网格用黑白两种颜色交替着色.在同一种颜色的每个三角形里取一个适当的点(但是略去

① 把一支点燃的蜡烛放在三个(无框镜子)之间,读者将看到一个非常优美的景象.明尼苏达大学曾把这个主意用于 Dihedral Kaleidoscopes 和 The Symmetries of the Cube 两个短影片里.

http://maths352.bokee.com

[redacted]

另一种颜色的三角形内相应的点)，我们就分别得到 3^6(又一次)，$3^4\cdot 6$ 与 $3^2\cdot 4\cdot 3\cdot 4$ 的诸顶点.(剩下的均匀拼砌 $3^3\cdot 4^2$ 不能由此类任何方法得到.)上图揭露了各种拼砌之间的许多关系：如 3^6 的诸顶点出现于 6^3 的诸顶点之中，6^3 的诸顶点三等分另一个 3^6 的诸棱，一个 4^4 的诸顶点平分另一个 4^4 的诸棱，等等.

如果把第三个镜子水平地放着而不要再竖立起来，即，两个铰连着的镜子立在第三个镜子上，则像的个数不再是无限多了. 事实上，有 $4n$ 个像，这里 π/n 是两个立着的镜子夹的角度. 当物点位于立着的镜子之一的面上时，诸像点两两重合而构成一
[156] 个 n 棱柱的诸顶点. 三个镜子两两所夹的三个二面角中有两个是直角. 一种自然的推广是这三个二面角是 $\pi/l,\pi/m,\pi/n$ 的情况.

由于用平面镜作反射时物点和像点总是和镜面成等距离的，容易看出这种推广的万花筒里所有的像点都处于同一个球面上，球的中心在三个镜面的交点上. 这些平面在这个球面上交出一个球面三角形，它的内角分别是 $\pi/l,\pi/m,\pi/n$. 所成的像平面把整个球面剖分为这样的三角形格网(或“地图”)，每个球面三角形包含着置放在第一个三角形内的物体的一个像. 所以像的个数等于球面三角形的个数，而所有的球面三角形在一起恰好是一个完整的球面. 取球面的半径为单位长，则整个球面的面积是 4π，而每个球面三角形的面积是 $(\pi/l)+(\pi/m)+(\pi/n)-\pi$. 所以球面三角形的个数是

$$4\Big/\left(\frac{1}{l}+\frac{1}{m}+\frac{1}{n}-1\right).$$

因为这个数必须是正的，所以必须选取 l,m,n，使它们适合

$$\frac{1}{l}+\frac{1}{m}+\frac{1}{n}>1.$$

这个不等式的解是 $2,2,n$；$2,3,3$；$2,3,4$；$2,3,5$. 第一种情况已经叙述过了；其余的情况画在第 165 页上(皮特里给出的).

我们必须知道，而且我们必将知道

http://maths352.bokee.com

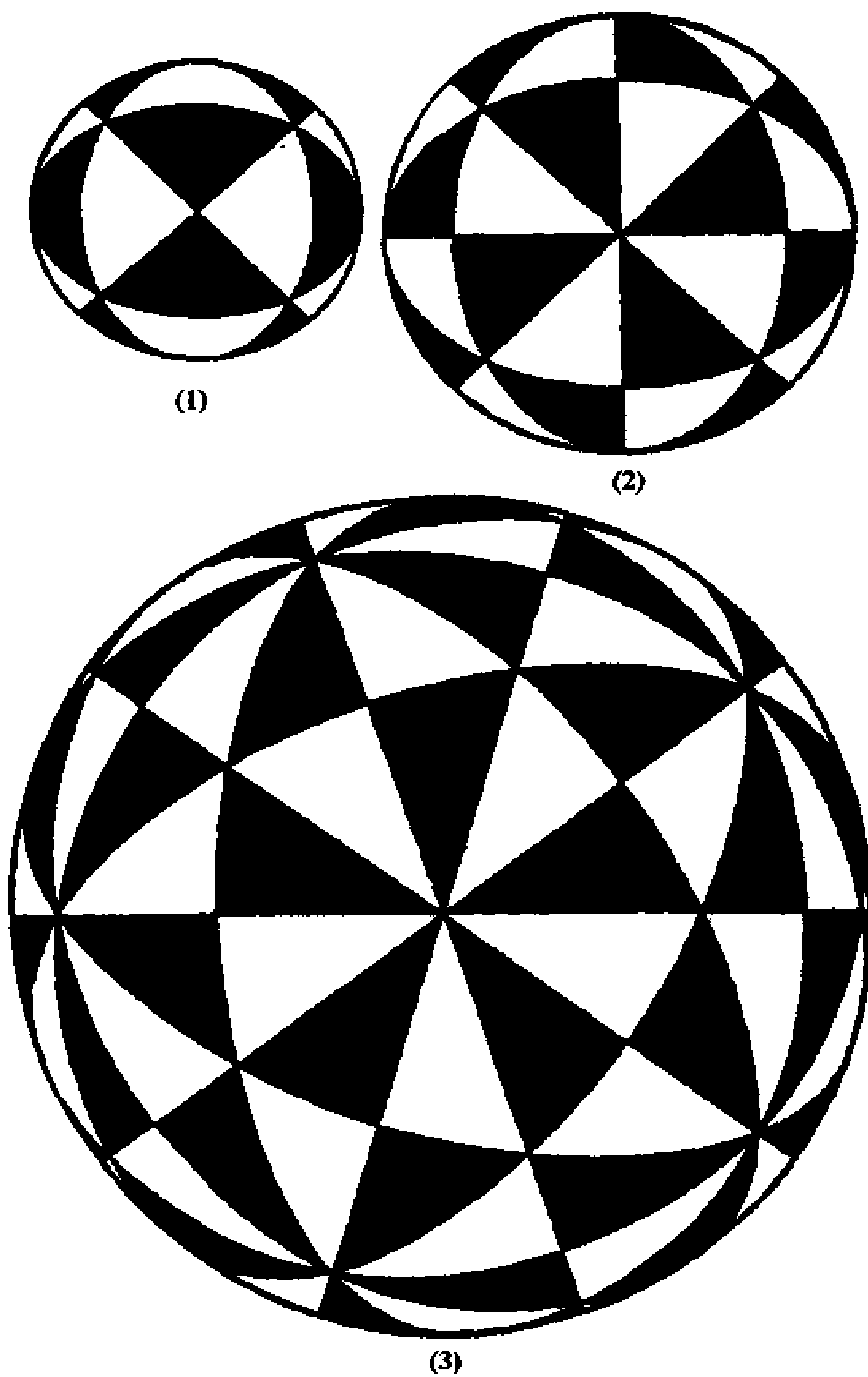


图 5.15 [158]

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

为了实际演示，在每种情况下都必须把镜子裁成半径相同(而且相当大)的扇形，它的圆心角①分别等于以 π/l，π/m，π/n 为内角的球面三角形的三个边长.

变动一个点物体在球面三角形内(或者说在三个镜面所成
[157] 的立体角内)的位置，就得到某些等角多面体的诸顶点.特别当点物体处于两个镜面相交所成的棱上时，或者在一个镜面上同时又和其他两个镜面成等距离时，或者在和三个镜面都相切的球面的中心上时，这个等角多面体的面都是正多边形.下图示明了各种匀称多面体发生②的样式，这和第 163 页上给出的关于平面拼砌的情况是类似的.

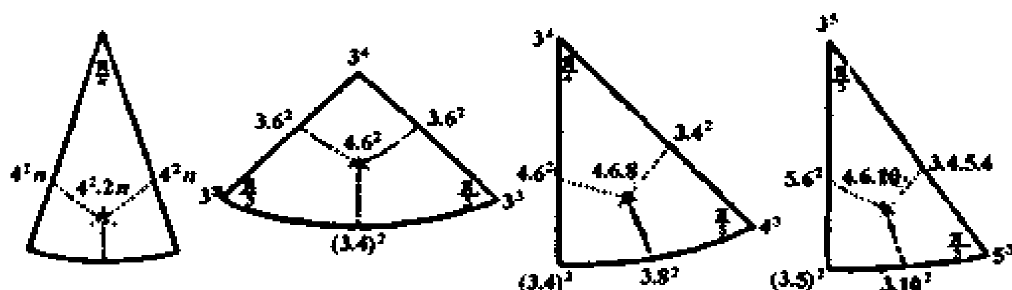


图 5.16

在每个白(或黑)色的三角形内取一个适当的点③，就会得到 $3^3 \cdot n$，3^5，$3^4 \cdot 4$ 或 $3^4 \cdot 5$ 的诸顶点.已经指出过狮鼻立方体 $3^4 \cdot 4$ 有构成一对的两种样子.其一的顶点都位于白色三角形

---

① 在这三种情况里，这些角分别是：55°44′，54°44′，70°32′；35°16′，45°，54°44′；20°54′，31°43′，37°23′.

② 参看 Möbius, Gesammelte Werke, 1861, Vol. Ⅱ, p.656，第 47，51，54 图；W. A. Wythoff, Proceedings of the Royal Academy of Sciences, Amsterdam, 1918, Vol. XX, pp.966—970; G. de B. Robinson, Journal of the London Mathematical Society, 1931, Vol. VI, pp.70—75; H.S.M. Coxter, Proceedings of the London Mathematical Society, 1935, series 2, Vol. XXXVIII, pp.327—339.

③ Möbius，见前注，第 46，49，53 图.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

内，另一个的顶点都位于黑色三角形内．狮鼻十二面体 $3^4\cdot5$ 也是这样．

再拿来第四个镜子，我们将得到空间拼砌．两两相交成 π 的几分之一角度的四个平面可以构出三种不同的四面体．可以从一个棱长为 $1\times\sqrt{2}\times\sqrt{2}$的长方体很方便地剖出它们来．设 $ABCD$ 是边长为$\sqrt{2}$的一个水平的正方形面．它在正方形 $A'B'C'D'$ 的正上方高为 1 处．用通过 A'，B，C'，D 四点之外的其他任意三点的平面分别把这四个顶点切掉，剩下的是四顶双楔形 $AB'CD'$，它就是所求的四面体之一．另一个是切下 [159]
来的任一个角上的块，如 $ABCB'$．（两个这样的块正好可以拼成和 $AB'CD'$ 相同的四面体．）第三个是用 $ABCB'$ 的对称平面 $BB'E$ 把它自己切开而得到的四面体，这里 E 是 AC 的中点．它的一半是 $AEBB'$．注意 AE，EB，BB' 是长度相等而又相互垂直的三条棱．

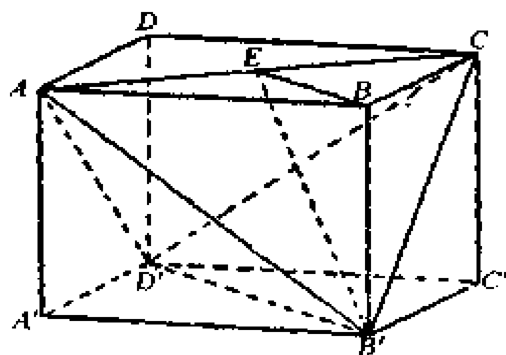


图 5.17

将一个点物体放到这种四面体的内部将会显出各种空间拼砌的顶点①，其中一些示于下边的图中（四面体 $AB'CD'$，$ABCB'$，$AEBB'$ 仍按原来的方位摆放）．

五个镜子可以围成一个三棱柱；这导致由棱柱嵌合成的

① Andreini，见前边第 154 页下的注③，第 17 至 24 图．

我们必须知道，而且我们必将知道

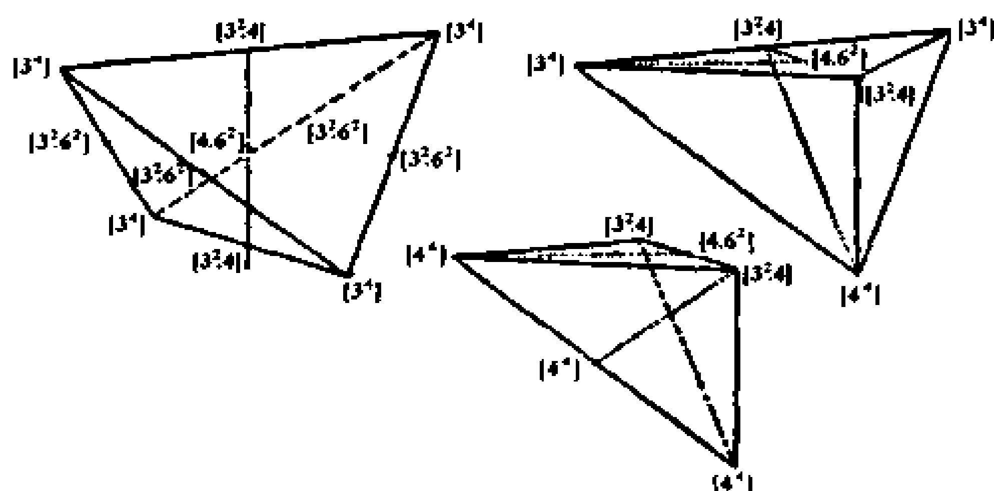


图 5.18

[160] 空间拼砌. 六个镜子可以围成一个长方体，其表面两两平行，就像在一个通常的房间里把天花板、地板、四壁整个都装上镜子一样；这就给出一种由长方块嵌合成的空间拼砌. G·波利亚(G. Pólya)①证明了任一种万花筒的功效和一个至多由六
[161] 面镜子做成的万花筒是相同的.

① Annals of Mathematics, 1934, Vol. XXXV, p.594.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第6章 棋盘上的游戏

棋类游戏是很好玩的.它们性质上多数属于几何学,然而其问题则是不同的一类,为数众多,宜立一章.有几个本来可以归入本章的问题已经在第4章里介绍过了.

18	28	38	48	58	68	78	88
17	27	37	47	57	67	77	87
16	26	36	46	56	66	76	86
15	25	35	45	55	65	75	85
14	24	34	44	54	64	74	84
13	23	33	43	53	63	73	83
12	22	32	42	52	62	72	82
11	21	31	41	51	61	71	81

图 6.1

普通的棋盘①包括64个小正方形,称为方格,共排列成8行与8列,如图6.1所示.这些格子通常被染上两种颜色——黑白交错或红白交错.可以用数字把它们编号,如11,12,等等,这里第一个数字表示方格所在的行,第二个数字表示方格所在的列.两个数字分别表示方格的中点的横坐标与纵坐标.以下就采

① 指国际象棋棋盘.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

用这种标号.一般的棋盘包括 n^2 个方格,排成 n 行和 n 列.我
[162] 要说的问题多数都可就具有 n^2 个方格的棋盘而论.

通常双方棋子各有王、后各一,象、车、马各两枚,还有八个兵.我假定读者是熟悉它们的走法的.

我要讲的不是棋弈本身和通常的胜负问题.各个棋子每走一步所形成的局势原则上是可进行数学分析的,但是一般地说来,下棋者可能走的步子太多了,因而要想预见长远的未来局势几乎是不可能的.这可以说是显然的,但不妨指出,要有实效地讨论对弈理论,其困难之大难以料想.已经计算过,仅是前四步的可能走法就有 197 299 种,前四步走后形成 71 782 种不同的可能局势,其中 16 556 种是当双方都只动"兵"的结果①.

棋子的相对威力

我要论述的第一个问题是确定各类棋子的相对威力②.一个放在某个方格上的棋子威力所及的格子的数目一般地说来取决于它的位置.我们可以把该棋子相继地放到棋盘的每个方格上去考察其威力所及的方格数,而把此种方格数的平均值作为对该棋子威力的评估.这和另一个说法是等价的,即,当把该棋子和一个王随机地下到棋盘上时,王受到将军的机率作为对该棋子威力的评估.如果未加其他限制,称这种将军为一简单将军.不论这个棋子先下到哪个方格上,王都可以下到其余 63 个方格的任一格上,而下到其中任一格上的机会是均等的.所以它受到将军的机率是该棋子威力所及方格的平均数的 1/63.

① L'Intermédiaire des Mathématiciens, Paris, December 1903, Vol. X, pp.305—308;又见 Royal Engineers Journal, London, August — November 1889;或 British Association Transactions 1890, p.745.

② H.M.Taylor, Philosophical Magazine, March 1876, *series* 5, Vol. I, pp.221—229.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

车在任一格上时的威力所及都共有 14 个方格.不论车放到哪个格上,王都还有 63 个格可占,而且这 63 个格被占的可能性 [163] 是一样的.所以出现简单将军的机率是 14/63,即 2/9.同样,在一个具有 n^2 个方格的棋盘上,这种机率是 $2(n-1)/(n^2-1)$,即 $2/(n+1)$.

马,当把它放在四角的任一格上时,如 11,威及两个方格;放在如 12 或 21 之类的 8 个格的任一格上时,威及三个方格;放在如 22 之类的 4 个格或如 13,14,15,16 之类的 16 个边格的任一方上时,威及四个方格;放在如 23,24,25,26 之类的 16 个格的任一格上时,威及 6 个方格;放在其余 16 个中部格的任一格上时,威及八个方格.所以马的威力所及方格的平均数是 $(4\times2+8\times3+20\times4+16\times6+16\times8)/64$,即,336/64.因此当一个王和一个马随机下到棋盘上时,王被简单将军的机率是 $336/(64\times63)$,即,1/12.同样,在具有 n^2 个格的棋盘上,这种机率是 $8(n-2)/n^2(n+1)$.

一个象放在 28 个边格的任一格上时威及 7 个方格;放在第二圈 20 个格的任一格上时威及 9 个方格;放在第三圈 12 个格的任一格上时威及 11 个方格;放在中部 4 个格的任一格上时威及 13 个方格.所以当一个王和一个象随机下到棋盘上时,王被简单将军的机率是 $(28\times7+20\times9+12\times11+4\times13)/(64\times63)$,即,5/36.同样,在具有 n^2 个格的棋盘上(n 为偶数),这机率是 $2(2n-1)/3n(n+1)$.当 n 为奇数时,由于棋盘上黑白两种方格不一样多,分析稍为复杂,但无特殊困难,此处不述.

在棋盘的任一个方格上放一个后时威力所及的方格和象与车的威力所及的方格的总和相同.所以,当一个王和一个后随机下到棋盘上时,王被简单将军的机率是 $(2/9)+5/36$,即,13/36.同样,在具有 n^2 个方格的棋盘上,当 n 为偶数时,这种机率是 $2(5n-1)/3n(n+1)$.

在上述假定下,车、马、象、后的相对威力是 8,3,5,13.据斯 [164]

我们必须知道，而且我们必将知道

http://maths352.bokee.com

汤顿(Staunton)编的《棋艺手册》,经验所得这组相对威力的真实比值是548,305,350,994;而冯·比尔格(Von Bilger)则认为是540,350,360,1 000,兵的相对威力取为100.

上述理论值与经验值之间的差距颇大.不过,有人认为相对威力的较合理的评估应该以把一个棋子和一个王随机地下到棋盘上时它能将王而不被王吃掉的机率.这种局势称为安全将军以别于简单将军.

应用上述分析方法,可算出安全将军的机率如下.对于车来说,安全将军的机率是$(4\times 12+24\times 11+36\times 10)/(64\times 63)$,即,$1/6$;在具有$n^2$个方格的棋盘上是$2(n-1)/n(n+1)$.对于马来说,一切将军都是安全的,所以其概率仍是$1/12$;在具有$n^2$个方格的棋盘上是$8(n-2)/n^2(n+1)$.对于象来说,安全将军的机率是$364/(64\times 63)$,即,$13/144$;在具有$n^2$个方格的棋盘上而$n$为偶数时是$2(n-2)(2n-3)/3n^2(n+1)$.对于后来说,安全将军的机率是$1036/(64\times 63)$,即,$37/144$;在具有$n^2$个方格的棋盘上当$n$为偶数时是$2(n-2)(5n-3)/3n^2(n+1)$.

按此种观点,车、马、象、后的相对威力是24,12,13,37;而斯汤顿的经验值的近似比为22,12,14,40,冯·比尔格的比值则近似于18,12,12,33.

同样的方法也可用于比较棋子组的威力.例如,双象(限一个占白格,另一个占黑格)和双车的简将的威力分别是$35/124$与$37/93$.所以在这种观点下,一个后要比双象的威力大而较双车的威力小.这与经验是符合的.

一个类似的问题是求把两个王随机地下到棋盘上时它们不
[165] 占相邻的方格——即谁也吃(能吃就吃)不掉谁——的机率.这个机率是$43/48$,因而它们占据相邻方格的机率是$5/48$.如果三个王随机地下到棋盘上,那么他们之中任何两个不占相邻方格的机率是$1\,061/1\,488$.在具有n^2个方格的棋盘上相应的机率分

我们必须知道，而且我们必将知道

http://maths352.bokee.com

别是①

$$(n-1)(n-2)(n^2+3n-2)/n^2(n^2-1)$$

和$(n-1)(n-2)(n^4+3n^3-20n^2-30n+132)/n^2(n^2-1)\cdot(n^2-2)$.

八后问题②

古典的与棋盘相关的问题之一是:要把八个后下到棋盘上(或者一般地把 n 个后下到具有 n^2 个方格的棋盘上)而任一个都不能吃掉其余的任一个,问有多少可能的下法.这个问题最初是1850年由弗朗兹·瑙克(Franz Nauck)提出来的.

炯特(Dr.S.Günther)③于1874年给出了一个利用行列式的解法.事实上,假定行列式的每个元素代表棋盘上的一个方格,那么一个具有 n^2 个方格的棋盘上的问题如果有解的话,这解应该由行列式

$$\begin{vmatrix} a_1 & b_2 & c_3 & d_4 & \cdots & \cdots & \cdots \\ \beta_2 & a_3 & b_4 & c_5 & \cdots & \cdots & \cdots \\ \gamma_3 & \beta_4 & a_5 & b_6 & \cdots & \cdots & \cdots \\ \delta_4 & \gamma_5 & \beta_6 & a_7 & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & a_{2n-3} & b_{2n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \beta_{2n-2} & a_{21-1} \end{vmatrix}$$

那种项给出,其中任何字母与下标都只出现一次.

---

① L'Intermédiaire des Mathématiciens, Paris, 1897, Vol. Ⅳ, p.6 与 1901, Vol. Ⅷ, p.140.

② 关于这个问题的历史可参看 W.Ahrens, Mathematische Unterhaltungen und Spiele, Leipzig, 1901, Chap. Ⅸ, 关于后来的发展情况,参看 Kraïtchik, La Mathématique des Jeux, Brussels, 1930, pp.300—356.

③ Grunert's Archiv der Mathematik und Physik, 1874, Vol. LVI, pp. 281—292.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

[166] 道理是明显的.行列式的每一项包含且只含每行的一个元素和每列的一个元素,所以任一项都表明一组方格,当 n 个后分占这些方格时它们彼此都不可能沿车路相互攻击.再者,在上列行列式中,字母和下标的安排的特点是:沿着任一象路看时,或者所有的字母都相同,或者所有的下标都相同.所以如果我们只挑选那些项,其中所有因子的字母都不同而且下标也都不同,则每一个这种项都表明这样一组方格,当 n 个后分占这些方格时它们彼此也不可能沿象路攻击.显然,行列式的项的正负号在这里是没用的.

在普通棋盘的情况下,相应的行列式是 8 阶的,它共有 8!即 40 320 项,所以除非发明出挑选所要的项的好办法,否则将这个办法用通常的 64 格棋盘或格子更多的棋盘实际是不可能的.

格莱谢尔(Dr. J.W.L.Glaisher)①于 1874 年提出过一个行之有效的办法,据我所知,这个理论迄今仍旧是他留下的那个样子.他证明了,如果在具有 n^2 个方格的棋盘上下 n 个后的问题的所有解都已经知道了,那么就可推出在 $(n+1)^2$ 个方格的棋盘上下 $n+1$ 个后的某一类解,而其余别的解也不难得出.只要用一个例子说明这个方法的应用就够了.

容易看出,当 $n=2$ 或 $n=3$ 时,问题无解.若 $n=4$,则行列式中有两项分别给出两个解,即,$b_2c_5\gamma_3\beta_6$ 与 $c_3\beta_2b_2\gamma_5$.为了求到当 $n=5$ 时的解,格莱谢尔是这样进行的.在这种情况下,炯特行列式是

$$\begin{vmatrix} a_1 & b_2 & c_3 & d_4 & e_5 \\ \beta_2 & a_3 & b_4 & c_5 & d_6 \\ \gamma_3 & \beta_4 & a_5 & b_6 & c_7 \\ \delta_4 & \gamma_5 & \beta_6 & a_7 & b_8 \\ \varepsilon_5 & \delta_6 & \gamma_7 & \beta_8 & a_9 \end{vmatrix}.$$

[167]

① Philosophical Magazine, London, December 1874, series 4, Vol. XLVIII, pp.457—467.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

为了得出那些包含 a_9 的解(如果有的话),只须把 a_9 添附到具有 16 个方格的棋盘的情况下的不含 a 的解上.由于上边所给的两个解都不含 a,所以得到两个解:$b_2c_5\gamma_3\beta_6a_9$,$c_3\beta_2b_6\gamma_5a_9$.据对称性,可以写出包含 a_1,e_5 与 ϵ_5 的解.这样得到的八个解都不相同;可以称之为第一类解.

以上所得的解都包含行列式四个角上的一个元素,这样的解只有那四个.其余别样的解可由下列行列式求之:

$$\begin{vmatrix} 0 & b_2 & c_3 & d_4 & 0 \\ \beta_2 & a_3 & b_4 & c_5 & d_6 \\ \gamma_3 & \beta_4 & a_5 & b_6 & c_7 \\ \delta_4 & \gamma_5 & \beta_6 & a_7 & b_8 \\ 0 & \delta_6 & \gamma_7 & \beta_8 & 0 \end{vmatrix}.$$

如果取这个行列式里与 b_2 相应的子行列式并把其中字母为 b 或下标为 2 的元素都换为零,那么就得到包含 b_2 的一切解.但这时这个子行列式仅有一项 $d_6a_5\delta_4\beta_8$,所以只有一个解:$b_2d_6a_5\delta_4\beta_8$.由对称性可得出包含 β_2,δ_4,δ_6,β_8,b_8,d_6,d_4 的解.容易看出这八个解中只有两个是不同的.可以称这些解为第二类解.

相仿地,剩下的解可由下列行列式得之:

$$\begin{vmatrix} 0 & 0 & c_3 & 0 & 0 \\ 0 & a_3 & b_4 & c_5 & 0 \\ \gamma_3 & \beta_4 & a_5 & b_6 & c_7 \\ 0 & \gamma_5 & \beta_6 & a_7 & 0 \\ 0 & 0 & \gamma_7 & 0 & 0 \end{vmatrix}.$$

如果在这个行列式里取与 c_3 相应的子行列式并把其中字母为 c 或下标为 3 的元素都换为零,那么就得到包含 c_3 的一切解.但是这个子行列式恒等于零,所以不存在包含 c_3 的解.据对称性可知也不存在包含 γ_3,γ_7 或 c_7 的解.如果有包括第一或末 [168]

我们必须知道,而且我们必将知道

http://maths352.bokee.com

一行(或列)的第三个元素的解,我们就称之为第三类解.

于是一共得到十个解,而且只有这十个解,它们是:八个第一类解,两个第二类解.

相仿地,若 $n=6$,则无第一类解,有 4 个第二类解,亦无第三类解.即,共有 4 个解.若 $n=7$,则得 16 个第一类解,24 个第二类解,无第三类解亦无第四类解,即共有四十个解.若 $n=8$,则得 16 个第一类解,56 个第二类解,20 个第三类解,即共有 92 个解.

注意,同一类型的解并非总是各异的.一般地,从任一个解可以立即推出另外七个解.这八个解中有四个是最初得到的解,或称为基本解,三个类似的解得自把棋盘转过一个、两个或三个直角,其余的四个是这四个在平面镜里的映象.但在任一特定情况下,映象可能不过是复制了原解,转过一个或两个直角也可能不产生新解.于是,在具有 $4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2$ 个方格的棋盘上分别有 1,2,1,6,12,46,92,341,1 784 个基本解,而总共的解数分别是 2,10,4,40,92,352,724,2 680,14 200.

下述基本解的集合想来读者是会感到兴趣的.各个后在棋盘上的位置都由一个相应的数码①表明.可是每一列方格上只能放一个后,因此我可以用一种较第 169 页上所说的更为简单的记法.这记法就是第一位数②表示在第一列方格上的后所占的方格从该列的一端数起所在的位置的编号,第二位数表示第二列上的这种编号,等等.如此,在具有 4^2 个方格的棋盘上的解
[169] 3 142的意义是在第一列第三格上、第二列第一格上、第三列第四格上、第四列第二格上各下一个后.如果一个基本解只引出四个解,我们就把表示它的数码用圆括号(　)把它括起来;如果它

① 参看 Thorold Gosset, The messenger of Mathematics, Cambridge, July 1914, Vol. XLIV, p.48.

② 从左端数起.但也可从右端数起.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

只引出两个解,我们就用括号〔 〕把它括起来;其他基本解各引出八个解,不再另加括号.

在具有 4^2 个方格的棋盘上,有一个基本解,即〔3142〕.

在具有 5^2 个方格的棋盘上,有两个基本解,即 14253,〔25314〕.注意循环解 14253,25314,31425,42531,53142 给五种可叠复的配位.如果将五个白后、五个黑后、五个红后、五个黄后、五个蓝后分别按此五种配位同时放到棋盘上,则颜色相同的后谁也不能吃掉谁.

在具有 6^2 个方格的棋盘上只有一个基本解,即,(246135).四个解是可以相互叠复的.在伦敦街头上曾经将这个问题作为游戏以一便士的票价招揽游客.游戏的形势是用一个木制的小棋盘,上边画着纵、横、斜线如图 6.2 所示,并且在标着圆点处各钻一个洞.要求游戏者把六个针各插入一个洞里而任何两个针都不许在所画的同一条直线上.

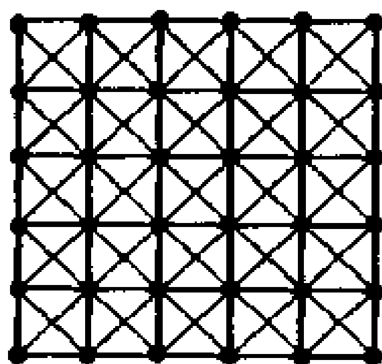


图 6.2

在具有 7^2 个方格的棋盘上有 6 个基本解:1357246,3572461,(5724613),4613572,3162574,(2574316).注意,将解 1357246 进行轮换就得到七个可叠复的解.

在具有 8^2 个方格的棋盘上,从某一角数起的第四个方格总 [170]
是要被占用的.12 个基本解是:41582736,41586732,42586137,42736815,42736851,42751863,42857136,42861357,46152837,

我们必须知道,而且我们必将知道

http://maths352.bokee.com

(46827135),47526138,48157263.这个排列次序是安德烈斯给出的.第七个解是唯一的任何三个后都不在一条直线上的解.要找到八个可叠复的解是不可能的①.但是我们能够按五种典型方法选出六个可叠复的解,其中有些还可以加上每组七个后的两个组,这样就用每组八个后的六个组和每组七个后的两个组填满64个方格中的62个格,其中任一个后都不能吃掉同一组中的其他子.这种解之一是:16837245,27368514,35714286,41586372,52473861,68241753,73625140,04152637.对于其他容量的棋盘也可以构成类似的叠复问题.

诺曼·安宁(Norman Anning)曾指出:这十二个基本解中有七个(第1,2,5,7,8,9,11个)可以在一个单行无限长的"缎子图案"上由适当选取八乘八的方块而找到.基本图案是由两直行四乘四的方块组成的,每行中的相连接的块都由一个马步相关联着.

在任何棋盘上由经验求解都无太大的困难.德灵顿(Mr. Derrington)已经造出下列解表:

2·4·1·3	4^2 格棋盘
2·4·1·3·5	5^2 格棋盘
2·4·6·1·3·5	6^2 格棋盘
2·4·6·1·3·5·7	7^2 格棋盘
2·4·6·8·3·1·7·5	8^2 格棋盘
2·4·1·7·9·6·3·5·8	9^2 格棋盘
2·4·6·8·10·1·3·5·7·9	10^2 格棋盘
2·4·6·8·10·1·3·5·7·9·11	11^2 格棋盘
2·4·6·8·10·12·1·3·5·7·9·11	12^2 格棋盘
2·4·6·8·10·12·1·3·5·7·9·11·13	13^2 格棋盘
9·5·7·3·1·13·11·6·4·2·14·12·10·8	14^2 格棋盘
15·9·7·5·3·1·13·11·6·4·2·14·12·8	15^2 格棋盘
2·4·6·8·10·12·14·16·1·3·5·7·9·11·13·15	16^2 格棋盘

① 参看 Thorold Gosset, The Messenger of Mathematics, Cambridge, July 1914, Vol. XLIV, p.48.

我们必须知道，而且我们必将知道



2·4·6·8·10·12·14·16·1·3·5·7·9·11·13·15·17　　17^2 格棋盘
2·4·6·8·10·12·14·16·18·1·3·5·7·9·11·13·15·17　　18^2 格棋盘
2·4·6·8·10·12·14·16·18·1·3·5·7·9·11·13·15·17·19　　19^2 格棋盘
12·10·8·6·4·2·20·18·16·14·9·7·5·3·1·19·17·15·13·11　　20^2 格棋盘
21·12·10·8·6·4·2·20·18·16·14·9·7·5·3·1·19·17·15·13·11　　21^2 格棋盘 [171]

等等.除了 n 的形式是 $6m+2$ 或 $6m+3$ 的情况外,规律是明显的.

最多子数问题

八后问题使人联想到多少有点类似的最多王数问题(或者更一般地,某种棋子的最多子数问题)——至多可以把几个王同时下到棋盘上而谁也不能吃掉谁,并且问有几种下法.

以王来说,这个数目是 16;例如,解答之一是把 16 个王下在如下的 16 个格子上:11,13,15,17,31,33,35,37,51,53,55,57,71,73,75,77.对于后来说,这个问题显然已被概括到前一段的分析里了,其数为 8.对于象来说,其数为 14,下子的位置是边上的方格;例如,解答之一是如下的 14 个格:11,12,13,14,15,16,17,81,82,83,84,85,86,87;共有 256 个解.对于马来说,其数为 32;例如,可以把它们都下在所有白格上或所有的黑格上,而且有两个基本解.对于车来说,其数显然为 8,共有 8!个解.

最少子数问题

另一个性质有些类似的问题是最少王数问题(或者更一般地,某种棋子的最少子数问题)——至少须把几个王同时下到棋盘上使所有的格子上的子都受到威胁.

以王来说,这个数目是 9;例如,可以把 9 个王下在方格 11,14,17,41,44,47,71,74,77 上.对于后来说,其数为 5;例如,可把它们下在方格 18,35,41,76,82 上.对于象来说,其数为 8;例如,可以把它们下在方格 41,42,43,44,45,46,47,48 上.对于马来说,其数为 12;例如,可以把它们下在方格 26,32,33,35,36,43,56,63,64,66,67 和 73 上,这些方格形成四组,每组三格,位

我们必须知道，而且我们必将知道

http://maths352.bokee.com

置对称.对于车来说,其数为8,八个解都是显然的.

[172] 还曾经讨论过当棋盘具有 n^2个方格的情况下最少的后数问题①,n 可以取各样的值.当 $n=2$或3时,只要一个后就足以威胁所有方格上的子了,而也只有一个基本解.当 $n=4$时,需要两个后;而基本解有三个,即,把它们下在方格11和33上,或12和42上,或22和23上,它们共给出12个解.当 $n=5$时,需要三个后,有37个基本解,共给出186个解.当 $n=6$时也只需要三个后,但只有一个基本解——三个后分别下在方格11,35,53上,共给出4个解.当 $n=7$时需要四个后,五个基本解之一是把它们下在方格12,26,41,55上.当 $n=8$时有638个基本解.

耶尼施(C.F.de Jaenish)还提出过这样的问题:求最少的后数,当把它们下在具有 n^2 个方格的棋盘上时,它们能威及所有的空格而任一个后不可能攻击其他的后.当 $n=4$ 时,这种问题须三个后,例如,把它们下在方格 11,23,42 上;共有两个基本解,总的解数为 16.当 $n=5$ 时,需要三个后,例如,可以把它们下在方格 11,24,43 上或 11,34,53 上;共有两个基本解.当 $n=6$ 时,需要四个后,例如,可以把它们下在方格 13,36,41,64 上;共有 17 个基本解.当 $n=7$ 时,需要四个后,只有一个基本解,即,已经说过的,下在 12,26,41,55 上,共给出 8 个解.当 $n=8$ 时,需要五个后,基本解不少于 91 个,例如,其中之一是把它们下在方格 11,23,37,62,76 上.

我把关于其他棋子的相应问题②——最少的棋子个数和可

① C.F. de Jaenish, Applications de l'Analyse mathématique au Jeu des Échecs, Leningrad, 1862, 附录自 244 页起;又见 L'Intermédiaire des Mathématicians, Paris, 1901, Vol. Ⅷ, p.88.

② L'Intermédiaire des Mathématiciens (Paris)里讨论过马的这种问题,见于 1896, Vol. Ⅲ, p.58;1897, Vol. Ⅳ, pp.15—17, 254;1898, Vol. Ⅴ, p.87, 230—231.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

能的解的个数——的讨论留给对此种问题感兴趣的读者. [173]

性质相同的另一种问题是求最少的后(或别的子)数,当把它们下到棋盘上时,它们能够相互保护并且威及所有其余的空格.以后来说,这个数目是5;例如,可以把它们下到方格24,34,44,54和84上.以象来说,其数为10;例如,可以把它们下在方格24,25,34,35,44,45,64,65,74和75上.以马来说,其数为14;例如,可以把它们下在方格32,33,36,37,43,44,45,46,63,64,65,66,73和76上;解是半对称的;还有另外两种安排.以车来说,其数为8,而解是明显的.怎样求各种情况下解的个数?我把这些问题留给对它们感兴趣的读者.

联系到这类问题,我可以谈谈另外两个性质相近的问题,是特顿上校引起我对它们的注意的.

第一个是要把八个后下到棋盘上使它们威及的格子尽量地少.譬如,把它们下在方格21,22,62,71,73,77,82,87上时,有十一个方格不会受到它们的攻击;还有别的下法,安全的方格也是十一个.这八个后是否可能有其他下法,使得安全的方格多于十一个?我从未找到那样的下法,但也一直未能证明其不可能.

另一个问题是要把m(m小于5)个后下到棋盘上使它们威及的方格尽量地多.例如,有好几种下法可以把四个后下到棋盘上使60个空格之中有58个受到威胁,只有两个是安全的;例如,可以把它们下在方格35,41,76,82上.自然可提出用别的子 [174]
的类似问题.

有说不尽的类似问题是关于各种棋子的组合的.例如,假定把四个后下在方格35,41,76,82上,那么除了两个空格之外其他的空格都受到威胁,这两个空格之一可以下上一个后,或一个王、一个车、一个象或一个兵而使另一个空格也受到威胁.假定把四个后下在方格22,35,43,54上,那么有三个空格是安全的,可以再把一个马下到这三个空格之一上而使其余两个空格受到威胁.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

棋盘上的回路

棋盘上的另一类问题是要用一个棋子走遍整个棋盘而且每个方格只许进入一次.

马的回路 先讨论古典的马的回路问题.关于这个题目的文献①太多了,我不打算全面地叙述解决这个问题的各种方法,而只想把我遇到过的关于某些解的几点注记写在这里,特别是德·莫瓦弗尔(De Moivre)、欧拉、范德蒙特(A.T. Vandermonde)、沃恩斯道夫(Warnsdorff)与罗热(P.M. Roget)所给的注记.

在一个具有偶数个格子的棋盘上,路线可能是巡回的,也可能不是,但在具有奇数个方格的棋盘上,它不可能是巡回的.因为如果一个马从一个白格上起步,它第一步必定走到黑格上,然后又走到白格上,如此等等.因此,如果它的路线经过所有的格子,那么在具有奇数个格子的棋盘上,最后一步须落在颜色和起步所在的格子相同的格子上,而这两个格子是不能用一个步子
[175] 连起来的.

我所知道的最早的解是18世纪初德·蒙特摩(De Montmort)与德·莫瓦弗尔②给出的那些.它们适用于通常具有64个方格的

---

① 关于文献书目,可参看 A. Van der Linde, Geschichte und Literatur des Schachspiels, Berlin, 1874, Vol. Ⅱ, pp.101—110.关于这个问题及其历史,参看沃尔皮契礼(P. Volpicelli)的文章,载于 Atti della Reale Accademia dei Lincei, Rome, 1872, Vol. XXV, pp.87—162;又见 C.F. de Jaenisch, Applications de l'Analyse mathématique au Jeu des Échecs, 3 Vols, Leningrad, 1862—3;以及 General Parmentier, Association Françise pour l'Avancement des Sciences, 1891, 1892, 1894.

② 这些方法是由它们的发明者寄给布鲁克·泰勒(Brook Taylor)的,问题好像是后者先前提出来的.我不知道它们被首先发表在什么地方;奥札南和蒙蒂克拉曾引用过它们;见 Ozanam, 1803版, Vol. Ⅰ, p.178;1840版, p.80.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

棋盘上，其关键是心中把棋盘划分成一个包括16个方格的中央正方形和一个两层格子组成的外环．如果开始时把马放在外环的某个格子上，就让它沿环顺着一个方向跳遍整个外环，只在绝对必要时才往中央跳一步．跳遍外环之后，再跳遍剩下的格子就不难了．如果开始时把马放在中央正方形的某个格子上，上述过程要颠倒过来．此法可用于各种大小的正方形或长方形棋盘．图6.3所示的德·莫瓦弗尔解，足以说明这个方法，其中格子里的数字表示跳进的顺序．我把它和另一个巡回问题的欧拉解并摆在一起，后者的棋盘是36个方格的方盘．如果真用棋子和棋盘作演示的话，最好每跳一步就把踏过的格子放上一个棋子．

34	49	22	11	36	39	24	1
21	10	35	50	23	12	37	40
48	33	62	57	38	25	2	13
9	20	51	54	63	60	41	26
32	47	58	61	56	53	14	3
19	8	55	52	59	64	27	42
46	31	6	17	44	29	4	15
7	18	45	30	5	16	43	28

图 6.3　德·莫瓦弗尔解

30	21	6	15	28	19
7	16	29	20	5	14
22	31	8	35	18	27
9	36	17	26	13	4
32	23	2	11	34	25
1	10	33	24	3	12

图 6.4　欧拉的36格解　[176]

在日内瓦的伯特朗(L. Bertrand)的建议下，欧拉①于1759年首先试探用数学方法对这个课题进行了严谨的分析，后来(1778年)伯特朗发表了一篇关于它的报告．这个方法可以用于任何形状和容量的棋盘，不过，一般情况下它导出的解都不是对称的，而且它们之间没有明显的联系．

欧拉从随便跳马开始，直到无处可跳为止．只要留点神，剩

① Mémoires de Berlin for 1759, Berlin, 1766, pp.310—337；或 Commentationes Arithmeticae Collectae, Leningrad, 1849, Vol. Ⅰ, pp.337—355.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

下的空格只不过几个.不妨记为 a, b,….他的方法就在于确立了一些规则,按照这些规则可以把这些空格插入到回路的各阶段中去,并使路线成为巡回的.

下边的例子说明这个方法,它是勒让德给出的,也是特别困难的例子之一.假定已经跳遍了图 6.5 中的路线,即,1,2,3,…,59,60,剩下没跳到的有四个空格,即,a, b, c, d.

55	58	29	40	27	44	19	22
60	39	56	43	30	21	26	45
57	54	59	28	41	18	23	20
38	51	42	31	8	25	46	17
53	32	37	a	47	16	9	24
50	3	52	33	36	7	12	15
1	34	5	48	b	14	c	10
4	49	2	35	6	11	d	13

图 6.5

22	25	50	39	52	35	60	57
27	40	23	36	49	58	53	34
24	21	26	51	38	61	56	59
41	28	37	48	3	54	33	62
20	47	42	13	32	63	4	55
29	16	19	46	43	2	7	10
18	45	14	31	12	9	64	5
15	30	17	44	1	6	11	8

图 6.6

我们先将路线 1 至 60 调成巡回的.格 1 控制着一个方格 p, p 是 32,52 或 2.格 60 控制着一个方格 q, q 是 29,59 或 51.
[177] 于是,如果 p 与 q 的这些值中有一对彼此的差为 1,那么就能把路线调成巡回的.若 $p=52$, $q=51$,情况就是这样.这时方格 1,2,3,…,51;60,59,…,52 就形成一个 60 步的巡回路线.因此,如果把数码 60,59,…,52 换为 52,53,…,60,步子的编号就成毗连的了.读者若想了解欧拉的议论细节,我建议你先把这个正方形画在纸上,然后再读下去.

然后,让我们把方格 a, b, d 添到这条路线里去.在上边调好的由 60 个方格组成的图里,被 a 控制的方格的数码是 51,53,41,25,7,5 和 3.选取哪一个都一样.假定选 51.这时我们必须使 51 成为 60 步路线的最后一步,那样就可以把 a, b, d 续上去了.为此,如果读者把图上的每个数码都加上 9,然后把 61,62,…,69 换为 1,2,…,9,你就得到一条由原号码为 60 的方格

我们必须知道,而且我们必将知道

http://maths352.bokee.com



开始的路线，而第 60 步就跳到原号码为 51 的格子，接下去第 61 步、第 62 步、第 63 步就可以依次跳进 a，b，d 了.

剩下的是再把 c 加入到路线中去. 因由 c 可跳进新号码为 25 的方格，而由 63 可跳进新号码为 24 的方格，所以此事可以仿上去完成. 具体地说，此时方格 1,2,…,24;63,62,…,25,c 构成一条马路. 因此应将号码 63,62,…,25 换成 25,26,…,63，然后在方格 c 里填写号码 64. 于是我们已经得到一条跳遍全盘的路线.

最后，还须将这路线调为巡回的. 首先须将方格号码 1 与 64 调近一些. 做法是：取由 1 可跳进的方格之一，如 28. 由 28 可跳进 1 和 27. 所以方格 64,63,…28;1,2,…,27 构成一条路线. 于是可以把编号 1,2,…,27 改为 27,26,…,1 而把这条路线图示出来.

现在，由方格 1 可跳进 26,38,54,12,2,14,16,28 号方格；由
64 号方格可跳进 13,43,63,55 号方格. 方格 13 与 14 是连步的，所 [178]
以方格 64,63,…,14;1,2,…,13 构成一条路线. 因此应把号码 1,2,…,13 改为 13,12,…,1，从而得到一条可以跳遍全盘的回路，见图 6.6. 欧拉说明过怎样由任一已知的回路导出另外七条回路.

用上述方法也不难构成由指定的方格开始并终止于另一指定的方格的一条路线.

欧拉进一步还研究过怎样改进他的方法，使之能用于解决带有附加条件的问题.

此类问题的一个有趣的例子是前 32 步限于在半个棋盘上走动. 解答之一绘示于图 6.7. 前 32 步的次序可用欧拉的方法确定. 显然，如果在这种步子的序码上都加 32，就得到跳遍另半个棋盘的由第 33 至第 64 步. 但是，一般地由 32 号格到 33 号格不是一个马步，由 1 号格到 64 号格也不是一个马步.

不过欧拉还说明了怎样确定前 32 步，使得当你把包括由 33
号格子到第 64 号格子的半个棋盘转过两个直角时，两半棋盘上 [179]
的路线变得连接起来并且是巡回的. 若从棋盘的两个相邻的边数起，某一方格处于第 x 行和第 y 列，则可称从棋盘的另两个对边

我们必须知道，而且我们必将知道

http://maths352.bokee.com

58	43	60	37	52	41	62	35
49	46	57	42	61	36	53	40
44	59	48	51	38	55	34	63
47	50	45	56	33	64	39	54
22	7	32	1	24	13	18	15
31	2	23	6	19	16	27	12
8	21	4	29	10	25	14	17
3	30	9	20	5	28	11	26

图 6.7　欧拉的半盘解

50	45	62	41	60	39	54	35
63	42	51	48	53	36	57	38
46	49	44	61	40	59	34	55
43	64	47	52	33	56	37	58
26	5	24	1	20	15	32	11
23	2	27	8	29	12	17	14
6	25	4	21	16	19	10	31
3	22	7	28	9	30	13	18

图 6.8　罗热的半盘解

数起，处于第 x 行和第 y 列的方格为其补格. 于是方格(x,y)与$(9-x,9-y)$为互补的，其中 x,y 分别表示前一方格所在的行数和列数. 在欧拉的解里，互补方格的编号之差为 32，例如方格(3,7)与(6,2)是互补的，一个的编号是 57，另一个的是 25.

后文所述的罗热法也可用于求半盘解，其结果如图 6.8 所示. 欧拉的文章的末尾阐明了怎样把他的方法用于十字形或其他长方形棋盘的问题上. 我特别要指出他的百个方格的正方形上的优美的巡回对称解.

下一步有意思的尝试属于范德蒙特①，他把问题化归为算术问题. 他的想法是用两个或更多的彼此无关的任意路线覆盖棋盘，然后把这些路线连起来. 他用一个分数 x/y 定义一个方格的位置，分子 x 是从棋盘的一个边数起的方格数，分母 y 是从棋盘的一个相邻的边数起的方格数；这就是说 x 和 y 是一个方格的坐标. 在表示一条马路的分数串里，两个相邻分数的分子的差只能是 1 或 2，而相应地分母的差必须是 2 或 1. 此外，x 和 y 都不能小于 1 也不能大于 8. 这个记法是很方便的，但范德蒙特仅用它去求得具有 64 个方格的棋盘上的问题的一个特解：他

① L'Historie de l'Académie des Sciences for 1771, Paris 1774, pp. 566—574.

我们必须知道，而且我们必将知道

用此法求解的做法和欧拉的做法很相仿,但只能用于具有偶数个方格的问题.按他的记法,他得到的路线是这样一串分数:5/5,4/3,2/4,4/5,5/3,7/4,8/2,6/1,7/3,8/1,6/2,8/3,7/1,5/2,6/4,8/5,7/7,5/8,6/6,5/4,4/6,2/5,1/7,3/8,2/6,1/8,3/7,1/6,2/8,4/7,3/5,1/4,2/2,4/1,3/3,1/2,3/1,2/3,1/1, [180]
3/2,1/3,2/1,4/2,3/4,1/5,2/7,4/8,3/6,4/4,5/6,7/5,8/7,6/8,7/6,8/8,6/7,8/6,7/8,5/7,6/5,8/4,7/2,5/1,6/3.

这条路线是巡回的,但是非对称的.如果把前三步移到这串分数的末尾去,他将会得到两条对称的回路,每条有 32 步,而连起来看却是不对称的,但还可能在这个问题上继续前进.范德蒙特还考虑过在一个立方体里的路线问题.

1773 年科尔里尼(Collini)①提出了限于用对称路线,其安排不考虑起始方格而以那样一种方式相连接,使我们能够从它起步.这是现代深究此类问题的基础.普拉特(Pratt)②于 1825 年、罗热于 1840 年各自再次发明了这个方法,后来许多作者都使用过它.但不论科尔里尼或者普拉特都未能巧用此法.后边将详述罗热所给的法则.

马路问题的最巧妙的解法之一是 1823 年沃恩斯道夫③所给的解法.他的法则是:马恒须跳进那种方格之一,在那里它能威及的未曾到过的方格数最少.所得的解不是对称的,也不是巡回的,而且实行起来也很不方便.这个法则未经证明其正确性,但也未发现其例外.它显然也可用于一切能被一个马跳遍的长

---

① Solution du Problème du Cavalier au Jeu des Échecs, Mannheim, 1773.

② Studies of Chess, 第 6 版,伦敦,1825.

③ H.C.Warnsdorff, Des Rösselsprunges einfachste und allgemeinste Lösung, Schmalkalden, 1823; see also Jaenisch, Vol. Ⅱ, pp. 56—61, 273—289.

http://maths352.bokee.com

方形棋盘.奇怪的是,在大多数情况下,跳错一步不影响结果,除非错误是发生在最后三四步中.

沃恩斯道夫还说过,当按法则马有两个或更多个方格可以跳进的时候,它可以跳进随便这些方格中的任一个.但事实并非如此,有人极为机智地构出了两三个失败的例子.不过出现这种
[181] 路线的情况是很少遇到的.

上述方法曾经用于各种形状的棋盘,特别是长方形的、十字形的和圆形的①.

一切新近的研究都假定了附加的限制:例如要求路线是巡回的,或者更一般地要求从指定的方格起步并终止于指定的另一个方格.

我所知道的最简单的解是德拉韦奈德(De Lavernède)的解,但更常称为罗热的解,后者于 1840 年发表的论文引起了对于它的广泛注意②.它把整个路线分成四个回路,可以将它们连接起来使我们能从任一个方格开始并终止于不同颜色的任一方格.于是,如果我们把马在起步时可以跳进的方格之一作为最后一个方格,那么就得到一条巡回的路线.另一方面说,这个法则仅适用于具有$(4n)^2$个方格的正方形棋盘.例如,它就不能用于法国人的棋子戏(jeu des dames),它有 100 个方格.

罗热先把 64 格的棋盘分成四个象限.每个象限有 16 个方格,这 16 个方格又分成四组,每组 4 个方格并构成一个闭合马路.这种闭路的每个方格都写上同一个字母,四个闭路分别用不

① 例如参见奇科里尼(T.Ciccolini)的著作 Del Cavallo degli Scacchi, Paris, 1836.

② J.E.T. de Lavernède, Mémoires de l'Académie royale du Gard, Nîmes, 1839, pp.151—179; P.M. Roget, Philosophical Magazine, April 1840, series 3, Vol. XVI. pp.305—309; 又见 Quaterly Journal of Mathematics, 1877, Vol. XIV, pp.354—359; 以及 Leisure hour, Sept. 13, 1873, pp.587—590, Dec. 20, 1873, pp.813—815.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



同的字母，譬如用 l,e,a 和 p. 写着辅音字母 l 的四个方格所成的闭路是菱形的，写着 p 的也是菱形的. 写着元音字母 e 的是正方形的，写着字母 a 的也是正方形的. 见图 6.9 中的任一个象限.

l	*e*	*a*	*p*	*l*	*e*	*a*	*p*
a	*p*	*l*	*e*	*a*	*p*	*l*	*e*
e	*l*	*p*	*a*	*e*	*l*	*p*	*a*
p	*a*	*e*	*l*	*p*	*a*	*e*	*l*
l	*e*	*a*	*p*	*l*	*e*	*a*	*p*
a	*p*	*l*	*e*	*a*	*p*	*l*	*e*
e	*l*	*p*	*a*	*e*	*l*	*p*	*a*
p	*a*	*e*	*l*	*p*	*a*	*e*	*l*

图 6.9 罗热解(i)

34	51	32	15	38	53	18	3
31	14	35	52	17	2	39	54
50	33	16	29	56	37	4	19
13	30	49	36	1	20	55	40
48	63	28	9	44	57	22	5
27	12	45	64	21	8	41	58
62	47	10	25	60	43	6	23
11	26	61	46	7	24	59	42

图 6.10 罗热解(ii)

现在，整个棋盘上写着同一个字母的 16 个方格可以连成一条回路，并且不论这回路从哪个方格起始，我们都可以让它终止于这回路的任另一格，只要它的颜色和起始格的不同就行. 如果 [182]
不计回路终止于哪个方格，那么我们就可使路线成为巡回的，并且沿每个小组(4 个方格)绕行的方向相同. 例如，上图 6.10 中用数码 1 到 16 标示着所有原来写着 p 的方格的巡回步骤. 相仿地，所有原来写 a 的方格组成标以 17 到 32 的回路，所有的 l 方格组成由 33 到 38 的回路，所有的 e 方格组成由 39 到 64 的回路. 这些回路都是对称而且巡回的. 辅音字母回路与元音字母回路算是两类异型的回路.

如果我们能够把这四条回路连成一条，并且从任一指定的方格起始而在第 64 步终止于指定的颜色不同的另一方格，那么一般问题就解决了. 为此，罗热给出了下列两条法则.

第一条. 如果起始方格与终止方格之一是辅音字母格而另一个是元音字母格，那么应交替地取辅音字母回路和元音字母回路，头一条回路就是起始格所在的回路，末一条回路自然应该

我们必须知道，而且我们必将知道

http://maths352.bokee.com

是终止格所在的回路.

[183] 第二条. 如果起始格与终止格都是辅音字母格或者都是元音字母格,那么先从终止格 Z 所在回路里选取一个由 Z 一步可达的方格 Y;其次再从异型的回路之一里选取一个由 Y 一步可达的方格 X. 这总是办得到的. 然后,暂且撇下方格 Z 与 Y,据第一条法则,总可以从指定的起始格经 62 步跳到方格 X;于是再跳两步就达到指定的终止方格 Z 了.

不论哪种情况,都必须注意在前三条回路的任一条上跳进时不要使棋盘角上的方格成为最后一格,最好也不要使棋盘边上的方格成为最后一格. 做到这一点是需要斟酌的. 只要合乎这些要求,就不难使路线成为巡回的且其走向和沿每组格子的绕行方向相同.

例 假定从 1 号方格(见图 6.10)起步,它是 p 回路之一中的方格,并且要想终止于 64 号方格,它是 e 回路之一中的方格. 情况属于第一条法则. 所以我们首先取写着 p 的 16 个方格,然后取写着 a 的 16 个方格,再取写着 l 的 16 个方格,最后取写着 e 的 16 个方格. 答案之一如图中所示. 因为马由 64 号格一步就能跳到一号格,所以路线是巡回的. 还有,图中的四条回路的每一条都是对称的,巡回的,且沿同一方向绕行. 仅只在由 32 号格跳进 33 号格时绕行的方向有明显的不一致.

后来许多作者都给出过与罗热法则类似的闭路法则,特别是德·波利尼亚克(A. de Polignac)[1]和拉奎埃(Lacquiére)[2],他们作了很详细的叙述,但似乎都未曾注意到罗热的法则. 德波利
[184] 尼亚克和罗热一样用在各个方格里写上字母的办法说明他的法

---

① Comptes Rendus, April 1861; Bulletin de la Société Mathématique de France, 1881, Vol. Ⅸ, pp. 17—24.

② Bulletin de la Société Mathématique de France, 1880, Vol. Ⅷ, pp. 82—102, 132—158.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

则，并且说有一个类似的法则适用于一切偶数个方格的情况.

罗热的方法还可用于两个二分棋盘，如第185页上的图6.8中所示.

耶尼施(Jaenisch)所给的最基本的方法与罗热的方法差不多.它有八种形式，与下边的图解相似，其中每行的或每列的数字的和都是260;但是，虽然它是对称的，依我看来，它不如罗热的方法好用.本书的前几版里还给出过一些别的解，值得注意的是穆恩(Moon)的解与文策莱德斯(Wenzelides)的解.下图中的两个回路每个包括32步，它们共同覆盖了棋盘.值得注意的是它构成了一个幻方①.

63	22	15	40	1	42	59	18
14	39	64	21	60	17	2	43
37	62	23	16	41	4	19	58
24	13	38	61	20	57	44	3
11	36	25	52	29	46	5	56
26	51	12	33	8	55	30	45
35	10	49	28	53	32	47	6
50	27	34	9	48	7	54	31

图 6.11 贾尼施的解

15	20	17	36	13	64	61	34
18	37	14	21	60	35	12	63
25	16	19	44	5	62	33	56
38	45	26	59	22	55	4	11
27	24	39	6	43	10	57	54
40	49	46	23	58	3	32	9
47	28	51	42	7	30	53	2
50	41	48	29	52	1	8	31

图 6.12 两个二分棋盘解

尚且不可能说出这问题有多少个解.勒让德②提到过这个问题，但最早试图解答它的是明金格(Minding)③.晚近的研究证明可能路线的数目小于④168件事物中每次取63件的组合数而 [185]
大于122 802 512，因为后者是一类特殊的回路的数目⑤.

① 见 A. Rilly, Le Problème du Cavalier des Échecs, Troyes, 1905.

② Théorie des Numbres, Paris, 第2版, 1830, Vol. Ⅱ, p.165.

③ Cambridge and Dublin Mathematical Journal, 1852, Vol. Ⅶ, pp. 147—156; Crelle's Journal, 1853, Vol. XLIV, pp. 73—82.

④ Jaenish, Vol. Ⅱ, p.268.

⑤ Kraïtchik, pp. 360, 402.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

类似的问题　可以提出类似的问题——要确定一个按某些规则而走的棋子(如王等)应采取的路线,使它从指定的方格走遍所有的方格或某些指定的方格,每格只走进一次而达于另一指定的方格.欧拉的方法可用于求此类路线.例如,他用自己的方法求到了一条走遍棋盘上黑色方格的回路,走子的规则是先像车一样走两格,接着再像象一样走一格.

王的回路①　图 6.13 是王的逐步走遍棋盘上每个方格的一条回路.我之所以想给出这么一个例子,是因为方格中表示先后次序的那些数字构成一个幻方.当然,这条路线也是后走遍棋盘的一个回路.

61	62	63	64	1	2	3	4
60	11	58	57	8	7	54	5
12	59	10	9	56	55	6	53
13	14	15	16	49	50	51	52
20	19	18	17	48	47	46	45
21	38	23	24	41	42	27	44
37	22	39	40	25	26	43	28
36	35	34	33	32	31	30	29

[186]　**图 6.13**　棋盘上王的幻方路线

车的回路　构造车的走遍棋盘的回路并无困难.例如,设开始时车在方格 11 中,它可以逐步走过方格 18,88,81,71,77,67,61,51,57,47,41,31,37,27,21 而回到 11.这是一条对称的路线.当然,这也是王或后的一条走遍棋盘的回路.如果我们从上列方格中的任一格开始,车总是用 16 步走完.如果从这些方

① 参看 I.Ghersi, Mathematica dilettevole e curiorsa, Milan, 1921, p.320 (fig. 261).

我们必须知道，而且我们必将知道

http://maths352.bokee.com

格之间的任一方格开始，那就要用 17 步才能走完这条路线．但是我相信在大多数情况下不论从哪个方格开始，16 步就足够了，不过一般地说，路线将不是对称的．在 n^2 个方格的棋盘上，要找到一条走遍所有其他方格（每格只经过一次）的车路也是可能的①．此外②，如果 n 是偶数，从任一格开始的车路都可以终止于不同颜色的任一其他方格中，如果 n 是奇数，那就可以终止于颜色相同的任一其他方格中．

象的回路　再举另一种例子．如果起步的方格选取得适当，那么象也可以用 17 步走遍棋盘上同一种颜色的方格③．例如，从方格 11 开始，可以相继经过方格 55，82，71，17，28，46，13，31，86，68，57，48，15，51，84，66，88．再有一步就可以回到起步的方格．于是象步的性质决定了有些方格它必须多次经过．

杂　　题

我们可以提出许多带有附加条件的走遍整个或部分棋盘的此类路线问题．这里再附上几个问题来考验一下不熟悉此类问题的读者．

各种路线问题　最简单的一个问题是要找一条车路，开始时它在方格 11 中，每步一格，每格只许进入一次，走遍全盘而最 [187]
后达到方格 88．这是可以做到的，不过我也曾见到过颇有素养的数学家在这个问题面前不知所措．粗心的读者很容易误解这个问题中的条件．

另一个简单的此类问题是要求把后从方格 33 用十五步走

---

① 未必．如 $n=3$ 而从 12 或 21 起步．——译者注

② L'Intermédiaire des Mathématiciens, Paris, 1901, Vol. Ⅷ, pp. 153—154.

③ H.E. Dudeney, The Tribune, Dec. 1906; Amusements in Mathematics. p.225.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



进方格 66,每格只许进入一次,路线不许交叉①.

一个类似的但比较难一些的问题是求后走的最长路线,从它的本位格出发,共走五步,进入过的方格不得再进入,且路线不许交叉②.计算路长时可假定路线通过方格的中心.如果每个方格的边长都是 1 寸,则路长大于 33.97 寸.

另一个熟知的问题提法如下:画 $m+1$ 条竖线和 $n+1$ 条横线,构成一个共有 mn 个格子.要从左上角沿格子线走到右下角,只许向下或向右走,问一共有多少可能的路线.答案是 $m+n$ 件事物的全排列数,事物中有 m 件是相同的一类,n 件是相同的另一类.这个数目是 $(m+n)!/m!n!$.在有 16 个方格的棋盘上(即国际象棋盘的四分之一),$m=n=4$,有 70 条这样的路线;在普通的棋盘上,$m=n=8$,这样的路线不少于 12870 条.车按同样的要求从左上角走到右下角有 $(m+n-2)!/(m-1)!\cdot(n-1)!$ 路线.对于长方形棋盘有类似的定理.

此类问题的另一个是:mn 个点排成 m 行 n 列.用纵线和横
[188] 线把它们连起来,构成一个四边形格网.求沿网线行走遍经所有这 mn 个点的闭路的条数,每点只许经过一次③.

瓜里尼(Guarini)问题 与棋盘有关的最古老的欧洲问题之一是1512年提出的下述问题.吕卡斯在1894年引述过它.但我相信除了在他的著作中和本书的前几版中之外,别处不曾公布

a	*C*	*d*
D		*B*
b	*A*	*c*

图 6.14

① H.E.Dudeney, The Tribune, Oct. 3, 1906.

② 前注,Oct.2,1906.

③ 见 C.F. Sainte-Marie in L'Intermédiaire des Mathématiciens, Paris, Vol. XI, March, 1904, pp.86—88.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

过.在上面画的只有九个方格的棋盘上,两个白马放在上边两角的方格(a,d)里,两个黑马放在下边两角的方格(b,c)里;其余的方格都空着.要求把白马跳进方格 b 和 c 里并且把黑马跳进方格 a 和 d 里.解法是显然的.

后的问题 另一个问题是要求把 16 个后下到棋盘上,但任何三个不得在一条直线上①.解答之一是把它们下在下列方格中:15,16,25,26,31,32,41,42,57,58,67,68,73,74,83,84.当然,棋子的位置都以方格的中心点为准.

拉 丁 方

一个 n 阶的拉丁方有 n 个不同的符号,每个符号有相同的 n 个,它们被排成一个方阵,并且每行或每列都是这 n 个不同符号的一种排列.如果取 $0,1,\cdots,n-1$ 为这些符号,把它们看成是模为 n 的同余类,那么一类特殊的拉丁方,记为$(1,1)_n$(如下边第一个例子),可以作为一个加法表(参看第 111 页)而构造

2	0	1
1	2	0
0	1	2

$(1,1)_3$

2	1	0
1	0	2
0	2	1

$(2,1)_3$

1	2	3	0
2	3	0	1
3	0	1	2
0	1	2	3

$(1,3)_4$

4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4
0	2	4	1	3

$(2,1)_5$

图 6.15

① H.E. Dudeney, The Tribune, November 7, 1906; Amusements in Mathematics, p.222.

我们必须知道,而且我们必将知道

http://maths352.bokee.com



[189] 出来.更一般些的是拉丁方$(\alpha,\beta)_n$,其最下边一行的数字是0,α,2α,…(按模n约简),最左边的一行是0,β,2β,…,其他方格中的数字是它对应的底行和最左列中数字的和(按模n约简).

显然,α和β必须与n互质.如果$\alpha+\beta$和$\alpha-\beta$也都与n互质(如图6.15中最后一个例子),那么该拉丁方必是对角形的,即每条对角线上的字符全不相同(每行或每列中的字符当然也都不相同).

相仿地,对于任一素次幂$q=p^k$和$GF(p^k)$的适合$\alpha\beta\neq0$的任两个元素,可以构造一个拉丁方$[\alpha,\beta]_q$,它同时也是α和β的倍数在那个伽罗瓦域中的一个加法表.如果$\alpha^2\neq\beta^2$,这拉丁方还是对角的.若$q=4$或9,我们可以把$GF(q)$的元素解释为q进位制的数,然后再把它转换为十进制.最后所得拉丁方和$(\alpha,\beta)_q$是不同的.

欧拉方 如果把两个n阶拉丁方叠合起来,这时得到的n^2个有序字符偶皆不相同,则称这两个拉丁方为*正交的*.所得的结果称为一个*欧拉方*或者"希腊拉丁方",它的每个方格里是一个有序字符偶.后一个名词是起源于把一个用希腊字母排成的方
[190] 阵和一个用拉丁字母排成的方阵拼合到一起而来的.但是还是在有序偶的前后两个位置上都用同一套n个字符比较方便.下列几个例子的第一个可记为$(12,11)_3$,因为左边的数码形成拉丁方$(1,1)_3$,右边的数码形成和它正交的拉丁方$(2,1)_3$.相仿地,第二个例子是$(12,21)_5$,第三个是$[1,10]_{2^2}$和$[1,11]_{2^2}$的结合,其中用2和3分别代替了元素10和11,就好像它们是二进制数似的.末一个四阶拉丁方可以看成是奥札南的幻方问题①的一个解:要把16张带人形的扑克牌(取自同一副)摆成一个正方形,其中任一行、任一列或任一对角线上的4张牌的花色和爵位都不许相同.

① Ozanam,1723年版,Vol.Ⅳ,p.434.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

22	01	10
11	20	02
00	12	21

34	41	03	10	22
13	20	32	44	01
42	04	11	23	30
21	33	40	02	14
00	12	24	31	43

12	03	30	21
31	20	13	02
23	32	01	10
00	11	22	33

图 6.16

更一般地，只要式 $\alpha\beta' - \alpha'\beta$ 的值与 n 是互质的，则拉丁方 $(\alpha', \beta')_n$ 和 $(\alpha, \beta)_n$ 就是正交的．由于 $\alpha, \beta, \alpha', \beta'$ 都必须与 n 互质，这个命题仅当 n 为奇数时才是对的．结果所成的欧拉方 $(\alpha'\alpha - \beta'\beta)_n$ 当 $\alpha \pm \beta$ 和 $\alpha' \pm \beta'$ 都与 n 互质时是对角的，上边的例子 $(12, 21)_5$ 就是这样．

相仿地，“伽罗瓦方”$[\alpha', \beta']_q$（它的阶数是 q 的素数次幂）和 $[\alpha, \beta]_q$ 当 $\alpha\beta' - \alpha'\beta \neq 0$ 在 GF(q) 里成立时是正交的．特别是，当 β 遍取 GF(q) 的非零元时，所得的 $q-1$ 个拉丁方都是相互正交的．例如，上述两个相互正交的两个对角拉丁方 $[1, 10]_{2^2}$ 和 $[1, 11]_{2^2}$ 都与 $[1, 1]_{2^2}$ 正交（但它不是对角的）．

然而，存在着四阶的拉丁方，它不与任何别的拉丁方正交，例如 $(1, 3)_4$（见 195 页）．这样的拉丁方称为*不可扩充的*． [191]

当给出一个 m 阶的和一个 n 阶的拉丁方时，不难构造一个 mn 阶的拉丁方．由于当 n 为任一奇数时拉丁方 $(1, 1)_n$ 和 $(1, 2)_n$ 是正交的，而当 $q = 2^k (k > 1)$ 时，$[1, 1]_q$ 和 $[1, 10]_q$ 也是正交的，所以存在着任何奇数阶和任何双偶数阶的欧拉方．

欧拉的官员问题　欧拉方之所以称为欧拉方是因为欧拉首先研究了单偶数①阶的正交拉丁方存在的可能性．二阶的显然是不可能的．1872 年，欧拉将 6 阶的情况表述如下：有 36 位军

① 此处“单偶数(Singly-even number)”指等于奇数的二倍的偶数，如 $6 = 2 \times 3, 10 = 2 \times 5, 14 = 2 \times 7$ 之类的偶数，而 4, 8, 12, 16, 20, … 则非．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

官，分属于6个团和6个不同的军衔，任两个人所属的团号和军衔都不全相同.是否能够把他们排成六行六列的方阵，要使每一行里的六位军官分属于6个团且各人的军衔都不同，每一列里也是这样？他猜想这是办不到的.118年之后，塔里证明了欧拉的这一猜想①.遗憾的是，欧拉还猜想10阶，14阶，……的此种方阵都是不可能的.关于这些猜想的驳斥，参看本书第2页的插图和第10章.

欧拉立方　一个n阶的拉丁立方可定义为用n种不同符号排成的立方阵，每种符号有n^2个，立方阵中每一行、每一列、每一竖都是这n种符号的一个排列.特例是，只要α,β,γ都与n互素，那么以n为模的三维加法表就是一个拉丁立方.只要行列式

$$\begin{vmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{vmatrix}$$

与n互素，三个这样的立方叠合起来就形成一个欧拉立方
[192] $(\alpha''\alpha'\alpha, \beta''\beta'\beta, \gamma''\gamma'\gamma)_n$.我们将在第224页上利用这样的一个立方.

① L. Euler, Verhandelungen Zeeuwsch Genootschap der Wetenschappen, 1782, Vol. Ⅸ, pp. 85—239, 或 Commentationes Arithmeticae, Leningrad, 1849, Vol. Ⅱ, pp. 202—361; G. Tarry, Comptes Rendus de l'Association Française pour l'Avancement de Science naturel. 1900, Vol. Ⅰ, pp. 122—123; 1901, Vol. Ⅱ, pp. 170—203. 又见 R. A. Fisher and F. Yates, Proceedings of the Cambridge Philosophical Society, 1934, Vol. XXX, pp. 429—507, 以及 Albert Sade, Annals of Mathematical Statistics, 1951, Vol. XXII, pp. 306—307.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第7章 幻 方

一个幻方就是用一些正整数排列成的一个正方形，它的每一行里、每一列里以及每条对角线上的数字的和都相同．如果这些正整数是从1到n^2的一切正整数，那么就说这个幻方是n阶的．在这种情况，不难算出每一行里、每一列里以及每条对角线上的数字的和都等于$\frac{1}{2}n(n^2+1)$．以下除非另行声明，我的论述中指的都是这种幻方——即，由从1开始的一些正整数构成的幻方．同样的条件也适用于由n^2个成等差级数的正整数构成的幻方．

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

图 7.1　$n=4$

15	10	3	6
4	5	16	9
14	11	2	7
1	8	13	12

图 7.2　$n=4$

按上述条件，用前16个正整数排列成如图7.1或图7.2的样子，它们都是四阶幻方，其每行、每列、每条对角线上的数字的和都是34．相仿地，后边图7.3与图7.17都是五阶幻方；图7.7是一个六阶幻方；图7.15与图7.18都是七阶幻方；图7.14，7.21，7.29，7.40都是八阶幻方；图7.23，7.30都是九阶幻方； [193]
图7.10是一个十阶幻方．

构造这些幻方是一种古老的游戏，在神秘观念与某些特殊数字联系在一起的时代，很自然地要研究此类排列．早在公元

我们必须知道，而且我们必将知道

http://maths352.bokee.com

前，中国人已经构造了一些幻方．它们的传入欧洲似乎归功于15世纪初康斯坦丁堡的摩绍普拉斯（Moschopulus）．著名的科尼利厄斯·阿格里帕（Cornelius Agrippa，1486—1535）构造出了3，4，5，6，7，8，9阶的幻方．他还把它们与占星术的七星——太阳、月亮、金星、木星、水星、火星、土星——配合起来．有时候人们把一个幻方刻在银盘子上当作避瘟符．还有一个幻方（即图7.1中的那个幻方）出现在阿尔伯特·丢勒（Albert Dürer）作于1514年的名画"忧郁"上，最下一行中间两格里的数字正好是作品完成的年代．幻方的数学理论的研究是17世纪在法国开始的．其后便成为许多国家里作者热衷的课题①．

采用以下的术语是方便的．数字所占的小正方形为*方格*．习惯上从上往下数为第一行、第二行、……，再从左往右数为第一列、第二列、……．第 h 行与第 $n+1-h$ 行为*互补*的行，列亦如是．位于第 h 行第 k 列的方格和位于第 $n+1-h$ 行第 $n+1-k$ 列的方格为*相互斜称的*．斜称的两个方格的位置是关于棋盘的中心点对称的．

任一高于二阶的幻方可以马上造出来．所用的方法视阶数 n
[194] 为奇数（即可表示为 $2m+1$）、单偶数（即可表示为 $2(2m+1)$）或双偶数（即可表示为 $4m$）而异．以下给出我所熟悉的简单法则．

奇数阶的幻方

当 $n=2m+1$ 时，n 阶幻方可按下述德·拉·卢拜尔（De la Loubère）②的法则编写出来．首先，将数1置于第一行中间的方

① 关于这个论题的历史概述及其有关文献目录见 S. Günther 的 Geschichte der mathematischen Wissenschaften，Leipzig，1876，第4章；W. Ahrens，Mathematische Unterhaltungen und Spiele，Leipzig，1901，第12章；以及 W.S. Andrews，Magic Squares and cubes，Chicago，1917.

② S. De la Loubère，Du Royaume de Siam（英译本），London，1963，Vol. Ⅱ，pp. 227—247．德·拉·卢拜尔于1687—1688年作为路易十四的特使去泰国学到了这个方法．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

格里.然后将相继的数按自然顺序置入平行于向右上方倾斜的斜线上,这时(i)当达到第一行时,下一个数应置入最下行的右邻列的方格里,就像把最下列移到了紧靠第一行的上边似的;(ii)当达到最右列时,下一个数应置入第一列的上邻行的方格里,就好像把第一列移到了紧靠最右列的右边似的;(iii)当达到一个已经填有数字的方格或者达到正方形的右上角时,下一个数应置入该方格正下方的相邻方格内,然后按上述法则继续进行填写.看一看图 7.3 就会明白这些法则,它就是按这些法则构造的一个五阶幻方.

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

图 7.3 $n=5$

31	43	00	12	24
42	04	11	23	30
03	10	22	34	41
14	21	33	40	02
20	32	44	01	13

图 7.4 $n=5$

为什么这样的正方形排列会是一个幻方?最好用一个特例来说明其中的道理,如取 $n=5$,这时先将所有的数字改用 5 进位表示(如果幻方是 n 阶的,就用 n 进位表示).为了简 [195]
化讨论,再把所有的数字减 1,这显然不影响幻方的性质.结果得到的就是图 7.4 中的幻方,也可以把它看成一个欧拉方①.由于每行或每列中都包含着 5 个可能的个位数与 5 个可能的进位数,所以行与列的幻方性质自动得到保证;主对角线亦然.另一条对角线上的进位数都是 2(一般地是 m),好像不妙,可是它们的和仍然是对的.此外,从 0 到 n^2-1 每个数都出现而且只出现一次.

① 参看第 196 页.颠倒各行的次序并轮换各列,就可以从(12.11)导出由德·拉·卢拜尔法则所得的欧拉方.

我们必须知道,而且我们必将知道



应用这个法则，读者可以轻而易举地编写一个三阶的幻方．这样的幻方称为“洛书”①，据传说是公元前 2200 年中国的皇帝禹给出的，许多东方的人民至今仍把它当作一个符咒来用．甚至在西方，也常在大型客轮的甲板上看到它，作为掷盘戏（或推盘戏）的得分依据．

单偶数阶的幻方

A	C
D	B

图 7.5

当 $n=2(2n+1)$ 时，可以按下述拉尔夫·斯特雷奇（Ralph Strachey）的法则②编写 n 阶的幻方．先将正方形分成四个大小相等的小正方形 A,B,C,D．用德·拉·卢拜尔的方法将由 1 到 u^2（$u=n/2$）的正整数在 A 里排成一个幻方，再将由 u^2+1 到 $2u^2$，由 $2u^2+1$ 到 $3u^2$，由 $3u^2+1$ 到 $4u^2$ 分别在 B,C,D 里排成幻方．显然，这
[196] 四个幻方合在一起看时各列数字之和都是相同的．将 A 的正中间行里从第二列起的 m 个方格、其他行里最靠左边的 m 个方格里的数字与 D 中相应的方格中的数字相互交换．然后再将 C 的最右边的 $m-1$ 列的每个方格中的数字与 B 中相应的方格中的数字相互交换．自然，整个正方形中各列的数字之和仍是相等的．现在它的各行与各条对角线上的方格中的数字之和仍然不变，因为这种构造方式等于先在 A,B,C,D 里都用由 1 到 u^2 的正整数填写成相同的幻方，然后将它们和一个用四个进位数 $0,u^2,2u^2,3u^3$（每个重复出现 n^2 次）作成的 n 阶幻方叠加在一起．每个正方形都是幻方，叠加的结果必然仍是幻方，而且这种做法保证了从 1 到 n^2 的每个正整数都出现而且只出现一次．

---

① D. E. Smith, History of Mathematics, Boston, 1925, Vol. Ⅱ, p.591.

② 这是他在 1918 年 8 月的一封信里告诉我的．

我们必须知道，而且我们必将知道

8	1	6	26	19	24
3	5	7	21	23	25
4	9	2	22	27	20
35	28	33	17	10	15
30	32	34	12	14	16
31	36	29	13	18	11

图 7.6 原先的四分正方形

35	1	6	26	19	24
3	32	7	21	23	25
31	9	2	22	27	20
8	28	33	17	10	15
30	5	34	12	14	16
4	36	29	13	18	11

图 7.7 最后的正方形 $n=6$

27 + 8	0 + 1	0 + 6	18 + 8	18 + 1	18 + 6
0 + 3	27 + 5	0 + 7	18 + 3	18 + 5	18 + 7
27 + 4	0 + 9	0 + 2	18 + 4	18 + 9	18 + 2
0 + 8	27 + 1	27 + 6	9 + 8	9 + 1	9 + 6
27 + 3	0 + 5	27 + 7	9 + 3	9 + 5	9 + 7
0 + 4	27 + 9	27 + 2	9 + 4	9 + 9	9 + 2

图 7.8 最后的正方形，$n=6$ [197]

图 7.6 和图 7.7 表明怎样用这个法则去构造一个六阶幻方.在图 7.6 中原先的四分正方形 A 中那些有待和 D 的相应方格中的数字互换的数字的下边都打上了横线；图 7.7 表示出最后得到的幻方；图 7.8 表明这些交换何以能够把那些进位数安排到适当的位置上，使得整个正方形成为一个 n 阶幻方.

17	24	1	8	15	67	74	51	58	65
32	5	7	14	16	73	55	57	64	66
4	6	13	20	22	54	56	63	70	72
10	12	19	21	3	60	62	69	71	53
11	18	25	2	9	61	68	75	52	59
92	99	76	83	90	42	49	26	33	40
98	80	82	89	91	48	30	23	39	41
79	81	88	95	97	29	31	38	45	47
85	87	94	96	78	35	37	44	46	28
86	93	100	77	84	36	43	50	27	34

图 7.9 原先的四分正方形，$n=10$

我们必须知道，而且我们必将知道

92	99	1	8	15	67	74	51	58	40
98	80	7	14	16	73	55	57	64	41
4	81	88	20	22	54	56	63	70	47
85	87	19	21	3	60	62	69	71	28
86	93	25	2	9	61	68	75	52	34
17	24	76	83	90	42	49	26	33	65
23	5	82	89	91	48	30	32	39	66
79	6	13	95	97	29	31	38	45	72
10	12	94	96	78	35	37	44	46	53
11	18	100	77	84	36	43	50	27	59

[198] **图 7.10** 最后的正方形，$n=10$

考虑到这种构造法是新颖的，我再增加两个图，用以说明这个规则在编写十阶幻方中的应用. 在图 7.9 里，正方形 A 与 C 中有些方格里的数字有待和正下方 D 与 B 中相应方格里的数字互换，它们的下边都打上了横线，图 7.10 表明这样得到的十阶幻方.

双偶数阶的幻方

一个与丢勒的幻方（见图 7.1）所差无几的四阶幻方（图 7.11）可以编写如下：先将正整数 1 至 16 按自然顺序分写到四行里，然后把对角线上的方格中的数字换为分别与它们互补的方格中的数字就行了. 这样的法则①也适用于任意双偶数阶的幻方，只要我们把每一由 4^2 个方格组成的子块的对角线上的方格中的数字都换成相应的在该子块中的补格中的数字即可. 图 7.13和图 7.14 表明了 $n=8$ 的情况.

---

① Kraïtchik, p. 176. 希思（R.V. Heath）曾经设计出类似的一套构造幻立方的法则.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

	2	3	
5			8
9			12
	14	15	

图 7.11

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

图 7.12　$n=4$

	2	3			6	7	
9			12	13			16
17			20	21			24
	26	27			30	31	
	34	35			38	39	
41			44	45			48
49			52	53			56
	58	59			62	63	

图 7.13

64	2	3	61	60	6	7	57
9	55	54	12	13	51	50	16
17	47	46	20	21	43	42	24
40	26	27	37	36	30	31	33
32	34	35	29	28	38	39	25
41	23	22	44	45	19	18	48
49	15	14	52	53	11	10	56
8	58	59	5	4	62	63	1

图 7.14　$n=8$　[199]

镶边幻方

应当提到构造任意阶幻方的另一个通用方法，它是弗雷尼克尔(B. Frénicle)给出的．按照这个方法，要构制 n 阶幻方可先构制一个 $n-2$ 阶幻方，在它的每个数字上加一个正整数，然后给它增一圈方格并在这些方格里填上其余的数，使其结果成为一个幻方．这样我们就能够从一个三阶幻方逐步扩大到 5，7，9，…阶的幻方，即一切奇数阶的幻方．同样，还能够从一个四阶幻方逐步扩大到一切更大的偶数阶幻方．

只要说明图 7.15 里的七阶幻方是怎样写出的，就明白这个方法了．首先，随便用什么方法造出内部的 $n-2$ 阶幻方，其每条线上的数字之和是 $(n-2)\{(n-2)^2+1\}/2$．在它的每个数上加 $2n-2$，于是每行、每列、每一对角线上的数字之和成为 $(n-2)\{n^2+1\}/2$．至此，尚未出现的数字是 $1,2,\cdots,2n-2$ 以及它们的补数 $n^2, n^2-1, \cdots, n^2-2n+3$．这些剩下的数字要放在

我们必须知道，而且我们必将知道

http://maths352.bokee.com



4(n − 1)个边格里，而且每一对互补的数字要放在内部正方形的每一行、一列或一条对角线的两端.这就使两端各增一格的每一行、一列和一条对角线上的数字之和成为 $n(n^2+1)/2$. 下一步还要使镶边上的每一行、每一列中的数字之和也是这么多，这是不难试着办到的. 只要有点耐心，一层层地进行镶边，任何阶
[200] 的幻方都可以造出来. 当然它还有这样的性质：如果把镶边一层层地剥掉，每次剩下的正方形都是幻方. 这是自修数学家们非常喜爱的一个方法.

46	1	2	3	42	41	40
45	35	13	14	32	31	5
44	34	28	21	26	16	6
7	17	23	25	27	33	43
12	20	24	29	22	30	38
11	19	37	36	18	15	39
10	49	48	47	8	9	4

图 7.15　一个镶边幻方，$n=7$

	1	2	3			
		13	14			5
			21		16	6
7	17	23	25			
12	20	24		22		
11	19			18	15	
10				8	9	4

图 7.16

有人曾提出过安排镶边方格中数字的法则①，不过大都不甚简便. 最近特拉弗斯(J. Travers)②提出了一个构造奇数($n=2m+1$)阶幻方的简便方法. 我不想作文字的叙述而宁可用上边的例子来表明它(实际上是作为一个多层镶边的幻方). 图 7.16 表明数字 $1,2,\cdots,m$； $m+1,m+2,\cdots,2m$； $2m+1,2m+2,\cdots,3m$； $3m+1,3m+2,\cdots,4m$ 应占的位置. 然后不难填入互

① 例如，D. E. Smith 与 Y. Mikami 合著的 Japanese Mathematics, Chicago, 1914, pp. 116—120；此书 120 页上的图中数字 8 与 29 应予交换.

② Education Outlook, 1936. 另一个好法则见于 R. V. Heath, Scripta Mathematica, 1936, Vol. Ⅳ, p.67.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

补数.读者可能有兴趣试一试看自已能否仿作出一个构造镶边的偶数阶幻方的法则①.

同阶幻方的个数

一个未解决的理论问题是要确定五阶(或任何更高阶)幻 [201]
方的个数.实质上,三阶幻方只有一个,虽然通过镜面反射和绕中心的旋转可表现为八种形式.四阶幻方有 880 个,通过反射和旋转,它们可以表现为 7 040 种不同的形式.五阶幻方的个数尚不确切知道.从前边图 7.4 中所示用卢拜尔法构造的幻方,我们可以得到 720 个形式不同的幻方,因为所用的五个个位数 0,1,2,3,4 可以有 5!种排列,而进位数 0,1,3,4 可以有 4!种排列,这就得到 2 880 个五阶幻方,不过其中只有 720 个是实质不同的.巴协给出过一个稍微不同的五阶幻方②,他把 1 放在中心格的紧邻上边,于是又可以得出另外 720 个实质不同的五阶幻方.可是,还有许多其他构造奇数阶幻方的法则.德·拉·伊尔(P.De la Hire)曾指出,用他那时所知道的方法,不计通过反射和旋转所得,就能构造 57 600 个实质不同的五阶幻方.考虑到后来的其他方法,已经知道五阶幻方的总个数要大大超过一千三百万.

对称幻方与泛对角幻方

除了要确定已知阶数的幻方的个数这个问题之外,我们完全可以说构造以上定义的幻方的理论已经足够成熟了.因而近来的研究目标主要放在构造满足其他附带条件的幻方上.曾有人建议这样的附带条件——任意两个相互斜称的两个方格中的

① J.Travers 已经给出编制偶数阶幻方的一个比较复杂的法则,Engineering Gazette, Aug. 13, 1938, p.6.

② 参看 Kraïtchik, p. 128.

我们必须知道,而且我们必将知道

http://maths352.bokee.com



数字之和皆等于 n^2+1.这样的幻方称为对称的(或相伴的)幻方.丢勒的幻方(图 7.1)是对称的;所有卢拜尔的幻方(如图
[202] 7.3)也都是对称的;还有按上述方法构造的双偶数阶幻方(如图 7.12 与 7.14)也都是对称的.不存在单偶数阶的对称幻方①.

最早提出的附带条件之一是要求幻方中沿断对角线上数字之和与沿通常的两条对角线上的数字之和相等②.这样的幻方称为泛对角的,又称为超幻方、至美幻方或魔幻方.

早在 11 或 12 世纪,在印度的克久拉霍(Khajuraho)就铭刻着一个泛对角的四阶幻方③.与之稍微不同的一个此类幻方载于本章图 7.2 中.它的每一行、列与两条对角线上的数字之和都是 34,而且由数字 15,9,2,8; 10,4,7,13; 3,5,14,12; 6,4,11,13; 3,9,14,8 与 10,16,7,1 所在的六条断对角线上的数字和也是 34.

由定义可知,如果把一个泛对角幻方沿着任两邻行或邻列之间的分界线剖开、交换所得两部分,则形成的仍是一个泛对角幻方.显然,经过这样的一次横的交换和一次竖的交换,可以任意指定把幻方中的某个数字换到某个方格中去.

我已经指出过本质上只有一个三阶幻方.这个幻方不是泛对角的,所以泛对角幻方的阶数必大于 3.此外,不存在单偶数

---

① C.Planck, The Monist, Chicago, Vol. XXIX, p. 308.

② 德拉伊尔、欧拉与索弗尔(J.Sauveur)都提到过此类幻方.弗罗斯特(A.H.Frost)在 Quaterly Journal of Mathematics, London, 1878, Vol. XV, pp. 34—49 上的文章再度引起了他们的注意,后来有一些作者讨论过它们的性质.除弗罗斯特的文章外,我还相当多地借用了 American Journal of Mathematics, Vol. XIX, 1897, pp. 99—120 上麦克林托克(E. McClintock)的一篇文章.

③ D.E.Smith, History of Mathematics, Boston, 1925, Vol. II, p. 594. 关于此类幻方的一般理论,参看 J.B.Roser and R.J. Walker, Bulletin of the American Mathematical Society, 1938, Vol. XLIV, pp. 416—420.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



阶的泛对角幻方[①]. 不可用 3 整除的奇数阶的泛对角幻方可以 [203]
用一种类似于德·拉·卢拜尔法则的法则构造出来. 当阶数是 3 的或 4 的整倍数时,也已经有新的法则去把它们构造出来.

880 个四阶幻方中有 48 个是泛对角的. 罗瑟与沃克(R.J. Walker)已经证明五阶泛对角幻方共有 3 600 个,七阶泛对角幻方有三千八百多万个,八阶泛对角幻方的个数在六万五千亿以上.

德·拉·卢拜尔法则的推广 为了方便,兹采用两个坐标来识别 n^2 个格子. 具体地说,末一行中从左到右的格子是 $(0,0)$, $(1,0)$, $\cdots$, $(n-1,0)$, 而最左一列中从下到上各格子是 $(0,0)$, $(0,1)$, $\cdots$, $(0,n-1)$. 于是格子 (x,y) 位于第 $n-y$ 行、第 $x+1$ 列. 本书第 201 页上的约定等价于将坐标依模数 n 约简,因而格子 $(n+x,y)$ 和 $(x,n+y)$ 与 (x,y) 是同一个格子.

在德·拉·卢拜尔方法里,数码由 1 到 2 的步子就是将两个坐标都增加 1,即,按"向量" $(1,1)$ 前进. 相仿地,由 n 到 $n+1$ 的"前进步"是按向量 $(0,-1)$ 前进. 显然,这个方法可以推广到按其他向量前进. 譬如从 ξ 到 $\xi+1$ $(\xi=1,2,\cdots,n-1)$ 的步子沿 (a,b) 前进,而由 $\xi'n$ 到 $\xi'n+1$ $(\xi'=1,2,\cdots,n-1)$ 的前进步沿 $(a+a',b+b')$ 前进. 于是由 1 到 $n+1$ 的步子就是沿

$$(n-1)(a,b)+(a+a',b+b')\equiv(a',b')\pmod n$$

前进;由 1 到 $\xi'n+1$ 的步子是 $(a'\xi',b'\xi')$;由 1 到 $\xi'n+\xi+1$ 的步子是 $(a\xi+a'\xi',b\xi+b'\xi')$.

设数字 1 的位置是在方格 (i,j) 里. 任意其他数字 s 的位置可以推知,为此可将 $s-1$ 按 n 进位表示为 $\xi'\xi$,也就是把 s 表示为 $\xi'n+\xi+1$,其中 ξ' 与 ξ 都是小于 n 的正整数或零.

应用向量 $(a\xi+a'\xi',b\xi+b'\xi')$,则要找的向量就是 $(i+a\xi+a'\xi',j+b\xi+b'\xi')$. 任何别的数,譬如说 $s+X'n+X$,它的位置必然不同. 因此同余式 [204]

① C. Planck,前注.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$$aX + a'X' \equiv 0, \quad bX + b'X' \equiv 0 \pmod{n}$$

必然蕴含 $X \equiv X' \equiv 0$.而这个结论成立的条件是 $ab' - a'b$ 与 n 互质.(在德·拉·卢拜尔的情况是 $ab' - a'b = -1$.)

如果 a, b, a', b' 也与 n 互质(因而非零),则此幻方的每行、每列的和皆相等,因为同一列中的数是形如 $a\xi + a'\xi' \equiv c$ 的同余式的 n 个解组(ξ 值与 ξ' 值的组合),c 取由 0 到 $n-1$ 各个值.同一行中的数也有相仿的关系.由于 a, b, a', b' 和 $ab' - a'b$ 都与 n 互质,n 必为奇数.不然,若 n 为偶数,则 a, b, a', b' 都必须是奇数,从而 $ab' - a'b$ 将为偶数.所以我们可以把 n 表示为 $2m+1$.

最后,我们来选取 i 与 j,使中数(middle number)($\xi = \xi' = m$)置于中心方格(m, m)里.这需要

$$i \equiv (1 - a - a')m, \quad j \equiv (1 - b - b')m.$$

(在德·拉·卢拜尔的情况里,$i = m, j = 2m$;所以 1 的位置在最上一行正中间的方格里.)由此可知幻方是对称的,即,在斜称方格(x, y)与$(2m - x, 2m - y)$里的两个数是互补的.这就保证了对角线上的数字之和与行和、列和也都相等,即,符合幻方的性质.

用符号$\begin{pmatrix} a & a' \\ b & b' \end{pmatrix}_n$记这个幻方是方便的.于是德·拉·卢拜尔的幻方是$\begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix}_n$,巴协的幻方是$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}_n$.以上我们证明了:只要 a, b, a', b' 和 $ab' - a'b$ 都与 n 互质,就能构造出一个这样的幻方.

如果 $a+b, a-b, a'+b', a'-b'$ 也都与 n 互质,那么这幻方还是泛对角的.这是因为,在一条广义对角线上的数字是形为 $(a \pm b)\xi + (a' \pm b')\xi' \equiv c$ 的同余方程的 n 个解组.当 n 为 3 的整倍数时,要适合所有这些条件是不可能的;对于这类情况,需要修正上述方法.

[205] 当所有这些条件都被适合时,上边得到的 i 与 j 的值使得

我们必须知道，而且我们必将知道

http://maths352.bokee.com

幻方既是对称的又是泛对角的.当然,随便把数 1 放在哪个位置上,幻方仍然是泛对角的.例如,取 n 为与 6 互质的正整数,则所有的条件都被 $\begin{pmatrix}1 & -1\\ 2 & -3\end{pmatrix}_n$ 满足.如此,要构成一个五阶的泛对角幻方(图 7.17),我们可以先把 1 放到任何一个方格里,然后继以四个马步,向右进一格并向上进两格,写上 2,3,4,5,直到遇上一个已被占用的方格.这时像车一样向下退一格,如上继续进行,直到填满所有的方格.再者,在幻方 $\begin{pmatrix}1 & 1\\ 2 & -3\end{pmatrix}_n$ 里,所有的数字都可按马步前进相继写出,如图 7.18 中那样;例外的情况是当 $n=5$ 或 5 的整倍数时,因为 $ab'-a'b=-5$.

7	20	3	11	24
13	21	9	17	5
19	2	15	23	6
25	8	16	4	12
1	14	22	10	18

图 7.17 (泛对角幻方)$n=5$

26	21	9	4	48	36	31
44	39	34	22	17	12	7
20	8	3	47	42	30	25
38	33	28	16	11	6	43
14	2	46	41	29	24	19
32	27	15	10	5	49	37
1	45	40	35	23	18	13

图 7.18 $n=7$

阿尔诺(G.Arnoux)方法① 如果图 7.17 与 7.18 中的数字统统都减 1 并用 $n(=5,7)$进位制表示,则立即可认出其结果就是欧拉方$(23,44)_5$ 与$(62,43)_7$.反之,每个由个位数偶 00,01,…,$(n-1)(n-1)$构成的欧拉方当把这些数偶解释为 n 进位制的数字时显然就成为一个幻方. [206]

此外,任一形为$(\alpha'\alpha,\beta'\beta)_n$ 的欧拉方(即便不是对角的欧拉方),当轮换其各行与各列使中数 mm 位于中心方格(m,m)

① G.Arnoux, Arithmétique graphique. Les espaces arithmétiques hypermagiques, Paris, 1894, p. 51.比较 Kraitchik, pp. 130—146.

我们必须知道，而且我们必将知道

里时，皆成为一个幻方；这是因为，这样的轮换使幻方成为对称的——即，它把互补的数送到方格$(m+x,m+y)$与$(m-x,m-y)$中去了．事实上，方格$(m+x,m+y)$里的数位与$m+\alpha'x+\beta'y, m+\alpha x+\beta y$同余$(\bmod\ n)$．（为了使数字由1跑到$n^2$而不是由0到$n^2-1$，只须在每个数上加1.）

另一方面，上述德·拉·卢拜尔法则的推广把数$(m+\xi')n+(m+\xi)+1$置入方格$(m+a\xi+a'\xi', m+b\xi+b'\xi')$里．如果同余式

$$x\equiv a\xi+a'\xi',\quad k\equiv b\xi+b'\xi',$$
$$\xi\equiv\alpha x+\beta y,\quad \xi'\equiv\alpha'x+\beta'y\quad(\bmod\ n)$$

是相容的，即，如果

$$a\alpha+a'\alpha'\equiv b\beta+b'\beta'\equiv 1 \text{ 且 } a\beta+a'\beta'\equiv b\alpha+b'\alpha'\equiv 0,$$

这两个方法将导致相同的幻方．在这些情况下，称$\begin{pmatrix}a & a'\\ b & b'\end{pmatrix}$与$\begin{pmatrix}\alpha & \beta\\ \alpha' & \beta'\end{pmatrix}$为“互逆方阵”，因为按方阵乘法，它们的积是$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}(\bmod\ n)$．事实上，这两个方法与坐标变换的两个方面相对应①．显然，命题a,b,a',b'和$ab'-a'b$与n互质和另一个命题$\alpha,\beta,\alpha',\beta'$和$\alpha\beta'-\alpha'\beta$与$n$互质是等价的．

当n与6互质时，我们能够选取$\alpha,\beta,\alpha',\beta'$，使$\alpha\pm\beta,\alpha'\pm\beta'$以及$\alpha,\beta,\alpha',\beta',\alpha\beta'-\alpha'\beta$都与$n$互质．于是幻方$(\alpha'\alpha,\beta'\beta)_n$不仅是对角的，而且还是泛对角的．（除非还要求额外的对称性质，不需要轮换各行与各列.）从这个观点来看，最简单的例子是$(12,21)_n$（见本书196页）．

[207] **马戈西安方法** 以下说明阿尔诺法的一个推广，利用它可

① O. Veblen, "On Magic Squares", Messenger of Mathematics, 1908, Vol. XXXVII, pp. 116—118.

我们必须知道，而且我们必将知道

以构造 4 的整倍数阶或 3 的奇倍数(但不是 3)阶的泛对角幻方.图 7.19 载的是幻方$(12,21)_4$(它不是正常的欧拉方,因为 2 能整除 4).虽然它原来的样子不是幻方,但若将所有的数码 2 与 3 互换,如图 7.20 所示,则其结果不但是一个幻方,而且实际还是一个泛对角幻方.图 7.2 所示为此幻方在十进制下的形状.

23	31	03	11
02	10	22	30
21	33	01	13
00	12	20	32

图 7.19

32	21	02	11
03	10	33	20
31	22	01	12
00	13	30	23

图 7.20

更一般地,设 α 为任一偶数①,则幻方$(1\alpha,\alpha 1)_{2\alpha}$当其数码 $\alpha,\alpha+1,\cdots,2\alpha-1$ 被换为 $2\alpha-1,2\alpha-2,\cdots,\alpha$ 时变成泛对角幻方.在同一行里的个位数是两个特定的数,每个重复 α 次.马戈西安(Margossian)的代换使这些两两的个位数的和都是 $2\alpha-1$.相仿地,同一列中的进位数也如此.按这个法则构成的一个幻方($\alpha=4$)示于图 7.21 中.

相仿地,形为$(13,31)_{3m}$的一个幻方(m 为奇数)当其个位数码$0,1,\cdots,3m-1$被适当地置换使它们在新的顺序中(每三行

74	63	54	43	04	13	24	33
05	12	25	32	75	62	55	42
76	61	56	41	06	11	26	31
07	10	27	30	77	60	57	40
73	64	53	44	03	14	23	34
02	15	22	35	72	65	52	45
71	66	51	46	01	16	21	36
00	17	20	37	70	67	50	47

图 7.21 一个泛对角幻方,$n=8$(8 进位) [208]

---

① 若 α 为奇数,则结论不成立,因为这时幻方中的数字会有相同者.事实上,$\alpha\beta'-\alpha'\beta(=\alpha^2-1)$将不是与 $n(=2\alpha)$互质的.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

35	48	52	65	78	82	05	18	22
04	17	21	34	47	51	64	77	81
63	76	80	03	16	20	33	46	50
32	45	58	62	75	88	02	15	28
01	14	27	31	44	57	61	74	87
60	73	86	00	13	26	30	43	56
38	42	55	68	72	85	08	12	25
07	11	24	37	41	54	67	71	84
66	70	83	06	10	23	36	40	53

图 7.22

35	47	50	85	67	70	15	27	00
14	26	02	34	46	52	84	66	72
83	68	71	13	28	01	33	48	51
30	45	57	80	65	77	10	25	07
12	24	06	32	44	56	82	64	76
81	63	78	11	23	08	31	43	58
37	40	55	87	60	75	17	20	05
16	22	04	36	42	54	86	62	74
88	61	73	18	21	03	38	41	53

图 7.23 一个泛对角对称幻方，$n=9$(九进位制表示)

一组，共 m 组)各列的数字之和皆相同．为此，m 个三数组中的
[209] $\frac{1}{2}(m-1)$组0,1,2; 3,4,5;…可保留不变，其余的三数组中有两组内部作逆向轮换而剩下的$\frac{1}{2}(m-3)$组各组内部颠倒次序．例如，对于一个十五阶幻方，可保留0,1,2,3,4,5不变，而将其余的数依次换为7,8,6; 11,9,10;14,13,12．特别当 $m=3$时，即，对于九阶幻方，我们可以轮换$(13,31)_9$的各行与各列使44进入中心方格(图7.22)，然后再把数码0,1,2,3,4,5,6,7,8依次换为1,2,0,3,4,5,8,6,7．所得幻方(图7.23)不仅是泛对角的①，而且还是对称的．

非相邻数字的幻方

虽然不可能用相邻数字构造出单偶数阶的泛对角或对称幻方，普朗克(C．Plank)②曾经设计出一个用几乎都相邻的数字构造此类幻方的方法．对于单偶数 n 阶幻方，他用了从 1 到 n^2+3 这些正整数，其中去掉“中数”$\frac{1}{2}n^2+2$ 与另外任意两个和为 n^2+4

① Arnoux, Arithmétique graphique, pp.152—154.

② The Monist (Chicago), 1919, Vol. XXIX, pp.307—316.

我们必须知道，而且我们必将知道

的数.特别是,他还能只去掉$\frac{1}{4}n^2+1$的整倍数.每行、每列、每条对角线上数字之和皆为$\frac{1}{2}n(n^2+4)$.此外,对于泛对角幻方,每个包括$\left(\frac{1}{2}n\right)^2$个方格的子正方块中的数字之和都是$\frac{1}{8}n^2(n^2+4)$.

图 7.24 与 7.25 表明了 $n=6$ 的情况,去掉的数字是那些 10 的倍数.

28	1	26	36	8	21
3	35	7	27	23	25
34	24	22	2	29	9
4	32	19	12	39	14
13	17	15	37	5	33
38	11	31	6	16	18

图 7.24 一个泛对角幻方,$n=6$

28	1	26	21	8	36
3	35	7	25	23	27
34	24	22	9	29	2
38	11	31	18	16	6
13	17	15	33	5	37
4	32	19	14	39	12

图 7.25 一个对称幻方,$n=6$ [210]

素数幻方 涉及非相邻数字的另一个问题是纯用素数构造幻方.下边第一个例子(图 7.26)是杜德尼给出的,第二个例子(图 7.27)是贝霍尔特和舒尔德海姆(C.D.Shuldham)给出的.塞尔斯(H.A.Sayles)和芒西(J.N.Muncey)①曾构造出了 5,6,…,12 阶的素数幻方.(注意,所有这些先生们都未意识到素数表里并未真正包含 1.)值得注意的是芒西的幻方里采用 1,3,5,7,11,…,827 而不曾遗漏中间的任何一个素数.

67	1	43
13	37	61
31	73	7

图 7.26

3	71	5	23
53	11	37	1
17	13	41	31
29	7	19	47

图 7.27

① The Monist, 1913, Vol. XXIII, pp.623—630.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



图 7.28 示明了任一四阶幻方的贝霍尔特一般形式①(若 $a=b=d-c=\frac{1}{2}(A-B-C+D)$,则幻方是泛对角的,若 $a+c=d=b-c$ 且 $A+C=B+D$,则幻方是对称的.所以,决不可能既是泛对角的又是对称的,因为那样的话就得要 $A-a=B$).若在下图里取 $A=13, B=11, C=37, D=41, a=10, b=18, c=24, d=-2$ 就得到图 7.27.

$A-a$	$C+a+c$	$B+b-c$	$D-b$
$D+a-d$	B	C	$A-a+d$
$C-b+d$	A	D	$B+b-d$
$B+b$	$D-a-c$	$A-b+c$	$C+a$

[211] 图 7.28

二 重 幻 方

对于 n 的某些值(不小于 8)可构造出那样的 n 阶幻方,当每个方格中的数都换成它的平方时,所得仍是一个幻方②.

这里给两个例子.图 7.29 是绍茨(M.H.Schots)③给出的一个八阶泛对角幻方.为了表明暗含的欧拉方,所有的数字都用 8

① Nature, 1910, Vol, LXXXIII, p. 368. 又见 J. Chernick, American Mathematical Monthly, 1938, Vol. XLV, pp. 172—175.

② 参看 L'Illustrations (May 29, 1897)上科科兹的论述.研究过这个课题的有塔里·波尔捷(B.Portier),科科兹·里利(A.Rilly),巴尔贝特(E.Barbette)和安德鲁斯(W.S.Andrews).里利在他的 Études sur les Triangles et les Carrés aux deux premiers degrés (Troyes, 1901)上给出了二百多个此类幻方.

③ Bulletin de la classe des Science de l'Académie royale de Belgique, 1931, pp. 339—361. 参看 Sphinx, 1931, p. 137. 注意,这不是一个泛对角的欧拉方,因为同一断对角线上的数码有重复的(虽然它们的和与行和或列和都相同).(个位数码与进位数码分开来看.——译者注)

我们必须知道，而且我们必将知道

http://maths352.bokee.com

进位制表示.将每个数都加 1,则每行或列的数字之和都是 260,它们的平方和是 11 180.图 7.29 是希思的九阶双重幻方,用的是九进位制.

17	50	43	04	32	75	66	21
31	76	65	22	14	53	40	07
00	47	54	13	25	62	71	36
26	61	72	35	03	44	57	10
45	02	11	56	60	27	34	73
63	24	37	70	46	01	12	55
52	15	06	41	77	30	23	64
74	33	20	67	51	16	05	42

图 7.29 一个泛对角双重幻方,$n=8$(用 8 进位制)

76	82	64	15	27	00	41	53	38
11	23	08	46	52	34	75	87	60
45	57	30	71	83	68	16	22	04
62	74	86	07	10	25	33	48	51
03	18	21	32	44	56	67	70	85
37	40	55	63	78	81	02	14	26
84	66	72	20	05	17	58	31	43
28	01	13	54	36	42	80	65	77
50	35	47	88	61	73	24	06	12

图 7.30 一个对称双重幻方,$n=9$(用 9 进位制)

三重幻方 若幻方中的数字分别换成它们各自的平方后,结果仍是幻方,而且分别换成它们各自的立方后,结果也是幻 [212]
方,则此种幻方称为三重幻方.三重幻方也曾有人研究过.卡扎拉斯(Cazalas)①找到了一个 64 阶的此种幻方.本森(W.H.Benson)上校(卡莱尔市,宾夕法尼亚州人)曾发现一个 32 阶的.

其他幻方问题

人们自然会联想到与幻方有密切联系的一些问题.下边是一些实例.

骨牌幻方 一副通常的多米诺骨牌共 28 张,由双零到双六.每张牌都是长度为宽度的二倍的长方形,牌面上分为两个小正方形.这 56 个小正方形里,有八个空白、八个一点、八个两点,

① J.J.A.M.E.Cazalas, Carrés Magiques au degré n, Hermann, Paris, 1934, p.114.

我们必须知道,而且我们必将知道

[redacted]

等等.问题是要布置这些骨牌使其56个小正方形形成一个7行7列的一个大正方形并在一边镶上一串7个空白小正方形,使每行、每列以及大正方形的对角线上的小正方形里的点数之和
[213] 皆等于24.图7.31给出了一个解答①.

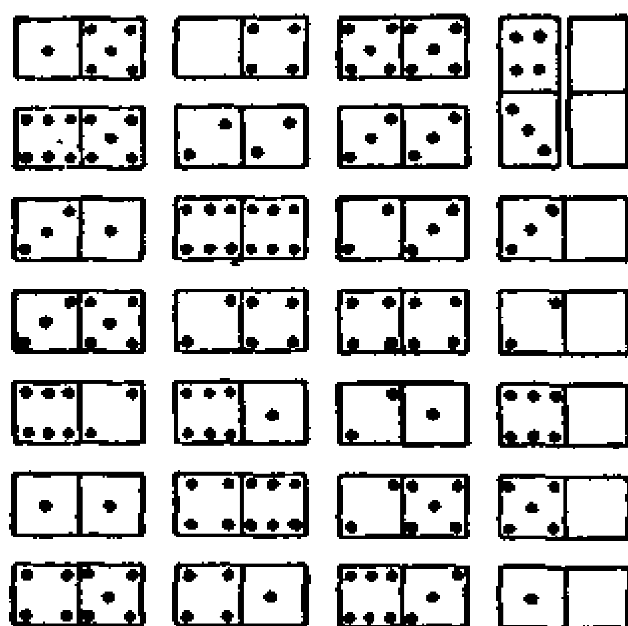


图 7.31 一个骨牌幻方

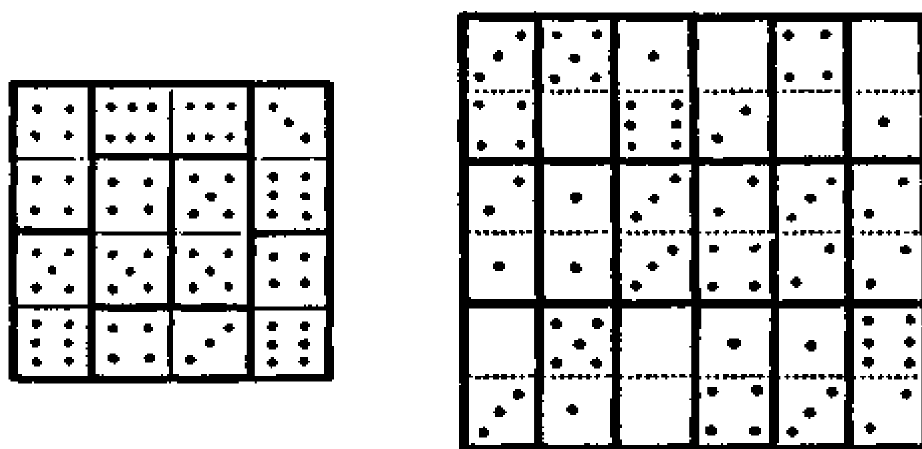


图 7.32 多米诺骨牌幻方

① 参看 L'Illustration, July 10, 1897; Scientific American, December 1969, Vol.221, no 6, pp.122—127.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

如果从一副骨牌里选出一部分牌而将其余的弃置不用，那么我们可以构造各种不同的幻方. 例如图 7.32 里所示的就是埃斯科特(E.B.Escott)与杜德尼给出的两个此类幻方.

正立方与正八面骰子 一个正立方体的六个面显然可以标上从 1 点到 6 点并使相背的两个面上的点数之和为 7. 这样附有标记的正立方体叫做骰子. 骰子常常成对地使用，但是似乎无人注意去规定作为一对的两个骰子应该是完全一样的呢或者是互为镜像的配对. [214]

另一种骰子可以这样做：把一个正多面体的 F 个面分别写上从 1 到 F 这 F 个数并使围绕每个顶点的各个面上的数字之和皆相等. 如果围绕每个顶点有 m 个面，那么这个和必须等于 $\frac{1}{2}m(F+1)$；因此，或者 m 是偶数，或者 F 是奇数. 每个正多面体的面数都是偶数，所以能够做成这种骰子的唯一的正多面体是正八面体($m=4$, $F=8$). 正八面体的面上的数字的安排(使围绕每个顶点的数字之和为 18)有三种本质上不同的方式，它们之中每一个皆有互反的配偶. 相背两个面上的数字之差为常数 1，或 2，或 4.

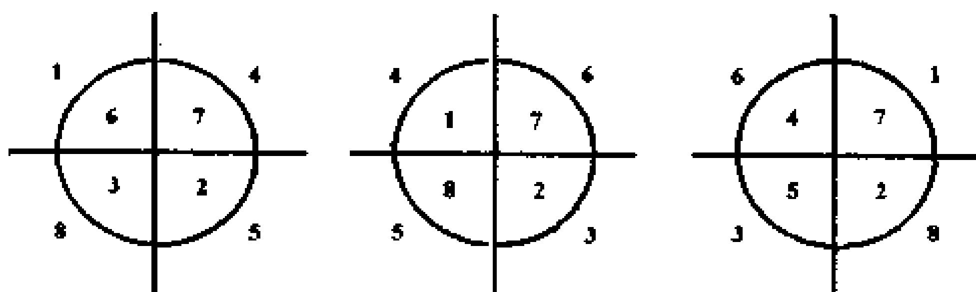


图 7.33 八面骰子①

联接六边形 在 n 个正四面体联接成的翻滚环(本书第 160 页)面上编号，要使围绕每个顶点的面上的数字之和都是

① 第三个骰子是安德烈斯给出的.

我们必须知道，而且我们必将知道

3(4n + 1)，这个问题好像是不可解的．然而，通过把环的每个面分成九块所得的 36n 个三角形网络的相应问题被 R·V·希思很漂亮地解决了．这样的三角形网络可以被看成环面(本书第 242 页)上的一个对称“地图”，即使 $n<6$ 也是一样．(当 $n\geqslant6$ 时，此“地图”可以按九种不同的方式画到翻滚环上．)图 7.34 示明最简单的情况($n=2$)，但有一个类似的方法①，它可以用于各种情
[215] 况．围绕任一顶点的六个三角形上的数字之和为 3(36n + 1)；和它们相邻的六个三角形上也是这样(它们构成一种星形)．希思做到了用此种联结的六边形去覆盖许多其他曲面．

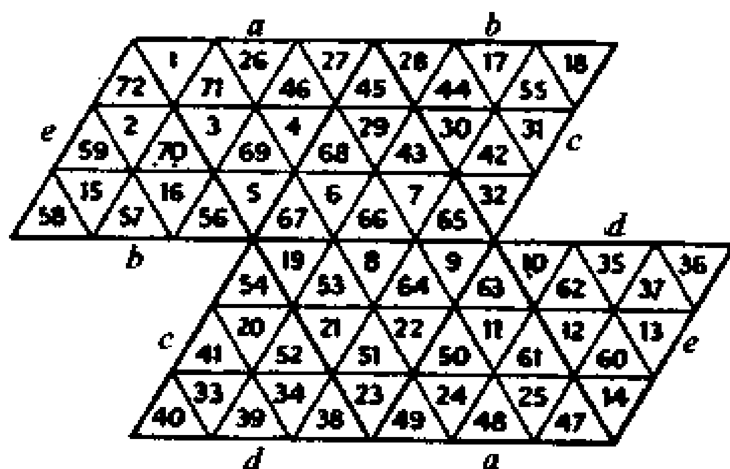


图 7.34　一个环体上的联接六边形

图 7.35 表明希思的特殊布置，他把数字从 1 到 32 分写到由八个正四面体连成的环的表面上．这些数字构成一个在完全不同的意义上的幻面．每个四面体的四个面上的数字之和都是 66；从每个四面体上取一个“位置相当”的面，这八个面上的数字之和都是 132(例如，9 + 7 + 17 + 31 + 10 + 8 + 18 + 32 = 132)；还有，呈螺旋状绕在环上的八个面上的数字之和也是132，这样的

① 此法与 n 为任一单偶数时完全相同．当 n 为奇数或双偶数时，两端须像图 7.35 里那样连接．在后一情况里，数字的正规安排在 9n 与 27n 之后遭到破坏．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

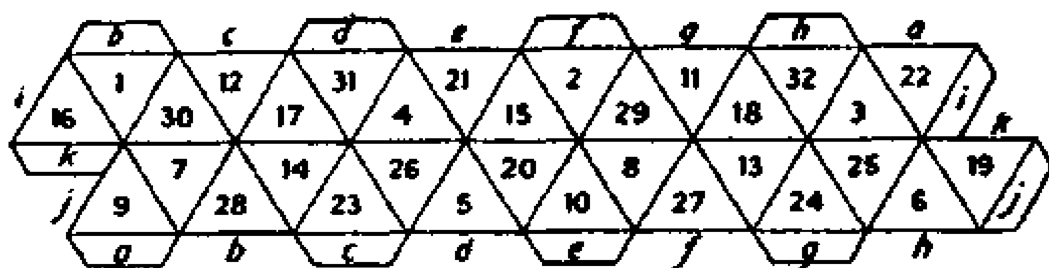


图 7.35 一个幻翻滚环

面组有八个(例如,1 + 12 + 31 + 21 + 2 + 11 + 32 + 22 = 132).

幻 立 方

n 阶幻立方由从 1 到 n^3 的所有正整数组成,它们被排列成一个正立方体的形状,而且要每行、每列、每竖以及四条对角线(或"直径")的任一条上的数之和皆相等. 这和就是 $\frac{1}{2}n(n^3+$ [216]
$1)$,共有 $3n^2+4$ 个这样的和. 我不知道有什么方法去构造单偶数阶的幻立方. 但是任何奇数阶的或双偶数阶的幻立方都有方法构造出来,这方法是构造幻方时曾用方法的一种自然推广.

像在二维的情况那样(本书第 209 页),我们一步一步地从一个方格走到另一个方格,只不过现在表示步子的向量都是三维的. 确切地说,我们规定步子(a,b,c)表示"向东"走 a 个方格,"向北"走 b 个方格,"向上"走 c 个方格. 和从前一样,所有的移动都是轮回的,所以数字 a,b,c 在任一阶段都可以按模 n 约简. 在到达一个被占用的方格之前,同样的步子可以走 $n-1$ 次. 然后走一个前进步$(a+a',b+b',c+c')$,接下去再走 $n-1$ 个(a,b,c)步,如此等等. 在直到要写 n^2+1 这个数字之前没有什么困难. 到了这个时候,前进步须改变为$(a+a'+a'',b+b'+b'',c+c'+c'')$,在达到 n^2 的每一个倍数之后都须改用一种新的前进步. 如果适当选取 a'',b'',c'',那么就会填满整个立方体. 事实上,数字 $\xi''n^2+\xi'n+\xi+1$ 的位置是从数字 1 经过 ξ 个(a,b,c)步,ξ' 个(a',b',c')步,ξ'' 个(a'',b'',c'')步而达到

我们必须知道，而且我们必将知道

的.如果 1 是在坐标为(i,j,k)的方格里,那么 $\xi''n^2+\xi'n+\xi+1$ 是在坐标为

$$(i+a\xi+a'\xi'+a''\xi'',j+b\xi+b'\xi'+b''\xi'',k+c\xi+c'\xi'+c''\xi'')$$

的方格里.

为了使不同的数总是占在不同的位置上,由同余式

$$aX+a'X'+a''X''\equiv 0,$$
$$bX+b'X'+b''X''\equiv 0,$$
$$cX+c'X'+c''X''\equiv 0 \pmod n$$

必须能推出 $X\equiv X'\equiv X''\equiv 0$.保证这个结论的条件是行列式

$$\begin{vmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{vmatrix}$$

[217]

与 n 互质.如能使所有的二阶子行列式都也与 n 互质,则各行、各列、各竖中数字之和皆相等.(若 n 为偶数,则这是不可能的.)要想使各条对角线上数字之和也都与行和相等,可调整 i,j,k,使中数落在中心方格里;这样一来,幻立方还是中心对称的.

(底层)			(中层)			(顶层)		
4	12	26	20	7	15	18	23	1
11	25	6	9	14	19	22	3	17
27	5	10	13	21	8	2	16	24

图 7.36 一个幻立方,$n=3$

采用符号

$$\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix}_n$$

去表示一个幻立方是方便的.上边说到,只要上述行列式及其二阶子式都与 n 互质,就能构造一个幻立方.显然,当 n 为任何奇数时,若

http://maths352.bokee.com

$$a = a' = b = b'' = c' = c'' = 1, a'' = b' = c = 0,$$

且 $i = j = k = \frac{1}{2}(n+1)$，则上述条件皆被满足. 实际构造幻立方时，最容易的是先将数 $1, n^2+1, 2n^2+1, \cdots$ 按步子 $(0,1,1)$ 填进去；其次将数 $1, n+1, 2n+1, \cdots$ 按步子 $(1,0,1)$ 填进去；最后将其余的数按步子 $(1,1,0)$ 填进去. 图 7.36 所示就是幻立方

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}_3$$

的三个"水平"层.

或许读者会有兴趣取 $n = 5$ 去试用一下这个法则. 结果所得幻立方是泛对角的，不仅它的四条主对角线上数字之和而且 [218]
所有断对角线上数字之和皆与行和、列和相等. 在这样的幻立方里，"幻和"发生 $(3+4)n^2$ 次而不是 $3n^2+4$ 次.

可以证明，只要 $a, b, a+b$ 与 $a^2 \pm ab \pm b^2$（包括正负号的四种配合）皆与 n 互质，则幻立方

$$\begin{pmatrix} a & b & 0 \\ b & 0 & a \\ 0 & a & b \end{pmatrix}_n$$

一定是泛对角的. 特别当 $a = b = 1$ 时，只要 n 不能被 3（也不能被 2）整除，就给出一个解；当 $a = 2, b = 1$ 时，只要 n 不能被 2, 3, 5, 7 中任一个数整除，就给出另一个解.

若 $a, b, a \pm b, a^2 + b^2$ 皆与 n 互质，则幻立方不一定是泛对角的，但其垂直于每个主方向的 n 个层都是泛对角幻方，所以幻和发生 $(3+6)n^2$ 次. 例如，$a = 2, b = 1$，则只要 n 与 30 互质，特别当 $n = 7$ 或更大的素数时，就给出一个解. 若 n 与 210 互质，特别当 $n = 11$ 或更大的素数时，这个幻立方自身将是泛对角的. 这时幻和发生 $(3+4+6)n^2$ 次. 罗瑟与沃克已证明了当 $n = 8$ 或 8 的任何倍数，以及 $n = 9$ 或任何更大的奇数时，一个幻

我们必须知道，而且我们必将知道

http://maths352.bokee.com

立方可以在这种严格的意义上是泛对角的，n 为别的数时都不行.

图 7.37 所示为与图 7.36 中所示的同一个幻立方，但其每个数字已减去 1 并用 3 进位制表示. 除了各层相轮换之外，这正是欧拉立方 $(122,212,221)_3$；因为包括 000 的行、列、竖包含 $GF(3^3)$ 的元 $\pm 122, \pm 212, \pm 221$，整个幻立方构成以这个行、列、竖为基础的加法表①. 由于

$$\begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1\end{pmatrix} \quad 与 \quad \begin{pmatrix}2 & 2 & 1\\ 2 & 1 & 2\\ 1 & 2 & 2\end{pmatrix}$$

互为逆阵(mod 3)，这两个构造法也对应着坐标变换的两个侧
[219] 面.

图 7.37 所示为立方 $(122,212,221)_4$（它不是真正的欧拉立方，因为 4 能被 2 整除）. 当每个数码 2 与 3 互换后，它变成一个幻立方，其结果用通常的记数法示于图 7.39 中. 实际上，当 α 为任一偶数时，马戈西安代换（本书 213 页）都给出一个泛对角幻立方 $(1\alpha\alpha, \alpha 1\alpha, \alpha\alpha 1)_{2\alpha}$.

010	102	221	201	020	112	122	211	000
101	220	012	022	111	200	210	002	121
222	011	100	110	202	021	001	120	212

图 7.37 一个欧拉立方，$n=3$

232	310	032	110	013	131	213	331	230	312	030	112	011	133	211	333
020	102	220	302	201	323	001	123	022	100	222	300	203	321	003	121
212	330	012	130	033	111	233	311	210	332	010	132	031	113	231	313
000	122	200	322	221	303	021	103	002	120	202	320	223	301	023	101

图 7.38 $n=4$

① Arnoux, Arithmétique graphique, p.63.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

60	37	12	21	7	26	55	42	57	40	9	24	6	27	54	43
13	20	61	36	50	47	2	31	16	17	64	33	51	46	3	30
56	41	8	25	11	22	59	38	53	44	5	28	10	23	58	39
1	32	49	48	62	35	14	19	4	29	52	45	63	34	15	18

图 7.39 泛对角幻立方，$n=4$

（第一层）　（第二层）

1	8	61	60	48	41	20	21
62	59	2	7	19	22	47	42
52	53	16	9	29	28	33	40
15	10	51	54	34	39	30	27
32	25	36	37	49	56	13	12
35	38	31	26	14	11	50	55
45	44	17	24	4	5	64	57
18	23	46	43	63	58	3	6

（第四层）　（第三层）

图 7.40 一个幻立它同时也是一个泛对角幻立方 [220]

图 7.40 是希思给出的，值得注意的是它既是一个八阶幻方，同时也是一个泛对角四阶幻立方．作为一个幻方，它有一个有趣的性质，即，在其任一行、任一列或任一对角线上的数字，每隔一个取一个，加起来都是 35．作为一个泛对角幻立方，它比图 7.39 中的幻立方更优美的地方就是它的每个水平层（它们是八阶幻方的四个象限）自身也都是幻方． [221]

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第8章 地图染色问题

本章和下一章涉及所谓拓扑学的一个数学分枝，它与几何学的不同之处在于它不牵涉到平直性与量度概念. 在这里每个卵形线都等价于一个圆，每个卵形面都等价于一个球面；实际上，如果一个图形经过挤压与拉伸之类的变换而能无破裂地变成另一个图形，则对这两个图形不加区别而认为它们是等价的.（这使人自然地联想到橡皮泥.）但是在拓扑学里是要区别球体与空心球，也区别它们之中任一个与环面或锚环. 它还区别一条简单闭曲线与一条纽结曲线，只要它们确切地被理解为存在于同一个三维空间里. 在四维空间里，任何这种纽结都可以被解开而无须弄断它.

四 色 猜 想

我首先叙述一个著名的猜想，表面上看来是很简单的，又似乎是对的，然而还没有被证明过，虽然这种类型的更复杂的定理的证明反而相当容易. 这猜想是：*要给一个国家的分省地图染色而任何两个相邻省份的颜色不得相同，为此至多四种颜色就够用了*. 这里，相邻省份的含义是：两个省至少有一段公共的分界线. 如果只有一个或几个公共的边界点，这些省就不算相邻的. 地图画在一个单连通面上，例如平面或球面. 省份的个数是有限的，任何一个省不能由两个或更多的地区组成. 地图可以覆盖整
[222] 个单连面，也可以只覆盖其一部分.（若地图是平面的并覆盖整

我们必须知道，而且我们必将知道

http://maths352.bokee.com

个平面，由于省份的个数是有限的，所以至少有一个省的面积是无限大．）当然，有些地图可以用少于四种颜色染成．例如一个国际象棋盘只需用两种颜色，一个六角形铺砌只需要三种颜色．

1853 年，伦敦的一个大学毕业生格思里（Francis Guthrie）①．在绘制英格兰的地图时觉察到只要用四种颜色就足以把所有的郡都区别开了．他意识到可能有个一般的定理，就和他的兄弟弗雷德里克（Frederick）讨论了这件事，后者向德摩根（De Morgan）教授请求给一个解释．德摩根对他的问题非常感兴趣，在致哈密尔顿（William Hamilton）爵士的一封信里提及了它，但是后来这个猜想的定理被人们遗忘了，直到 1878 年，凯莱②说到他未能作出它的严格证明．

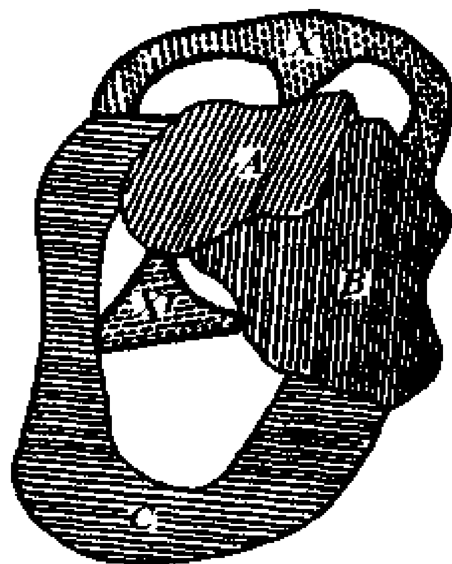


图 8.1

① Proceedings of the Royal Society of Edinburgh, July, 19, 1880, Vol. Ⅹ, p.728.

② Proceedings of the London Mathematical Society, 1878, Vol. Ⅸ, p. 148; Proceedings of the Royal Geographical Society, London, 1879, N.S., Vol. Ⅰ, pp. 259—261，其中指出了一些困难之所在．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

下边的论述虽然不是一个正式的证明，也许会使读者确信其结论的真实性.设 A，B，C 为三个相邻的区域，X 为和它们都
[223] 相邻的任意另一个区域.那么 X 必整个位于 ABC 区域的外边界之外，不然则整个位于其内边界以内，即，它必占有或者像 X 或者像 X' 的位置.不论哪种情况，都不可能再画出另一个区域 Y 使它与 A，B，C，X 都相邻.换句话说，在平面上画四个彼此都相邻的区域是可能的，但画五个这样的区域是不可能的.如果 A，B，C 不是两两相邻，或者 X 不与 A，B，C 相邻，那么就无须把它们染成都不相同的颜色.所以，最要紧的还是上边已讨论过的情况.此外，上述区域中的任一个都可能退缩为一个点以致于消失而不影响论述.

从图 8.1 显然可见，至少需要四种颜色，因为在图示的情况下，区域 A，B，C，X 需要染以不同的颜色.

这命题的证明有高度的困难，试图克服它们的道路至今都被阻塞了①.这部分地是由于这样一个事实：如果我们只用四种颜色去给地图上的区域一个一个进行染色，每当增入一个区域时都给它选定一种颜色，但是总能设法增入两三个那样的新区域，无法给它们染上与其邻接区域都不相同的颜色，于是只好推翻原来的染色方案；然而如果从头再来，又似乎总能调整我们的着色方案使此类新的区域可以染上适当的颜色.

肯普(A. B. Kempe)②于 1879 年给出了一个论证，从前人

---

① 美国数学家阿佩尔(K. Appel)和哈肯(W. Haken)于 1976 年用伊利诺斯大学的 IBM360 计算机运转 1 200 小时，分析了 1 482 种情况，从而给出了证明.但还期待着谁能作出简洁的证明.——译者注

② 他把他的原证投寄给大西洋彼岸的 American Journal of Mathematics，1879，Vol. Ⅱ，pp.193—200；后来又将其论证的简化形式递达 London Mathematical Society，Proceedings，1879，Vol. Ⅹ，pp.229—231，和 Nature，Feb. 26，1880，Vol. XXI，pp.399—400. P.J. Heawood 指出了论证中的毛病，见 Quaterly Journal of Mathematics，1890，Vol. XXIV，p.337.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

们都以为这个命题算是被证明了,殊不知其中有一点毛病.

彼得森图

泰特于 1880 年发表了一个以图论为基础的论证方法①.一个图(从图论的观点看)本质上就是一些点的配置,称这些 [224] 点为顶点,其中有些点偶由线段连接着,这些线段称为边(它们不一定是直的线段).设想图是绘于三维空间里的,我们可以保证任何两条边皆"不相交"而至多在同一个顶点相遇.一个多面体的顶点与棱就是这种例子.图也出现于电工里和化学中的分子结构式里.后一种应用使人们自然地称汇于一个点的边数为价,因而如果汇于每一个点都有三条边则称此图为三价的.在这种特殊情况下,顶点与边的数目显然是 $2n$ 与 $3n$,n 为某个正整数.

我们限于考虑连通图.所谓连通的含义是从图的任一顶点可沿着由一连串相邻的边组成的路径到达其他任一顶点.如果把一个边去掉后,整个图就分离为不相连通的两个部分,则称此边为一个桥(或地峡).如果一个图可以画在一张平面或一个球面上而且所有的边除了顶点外都无其他交会之点,则称之为一个平面图.

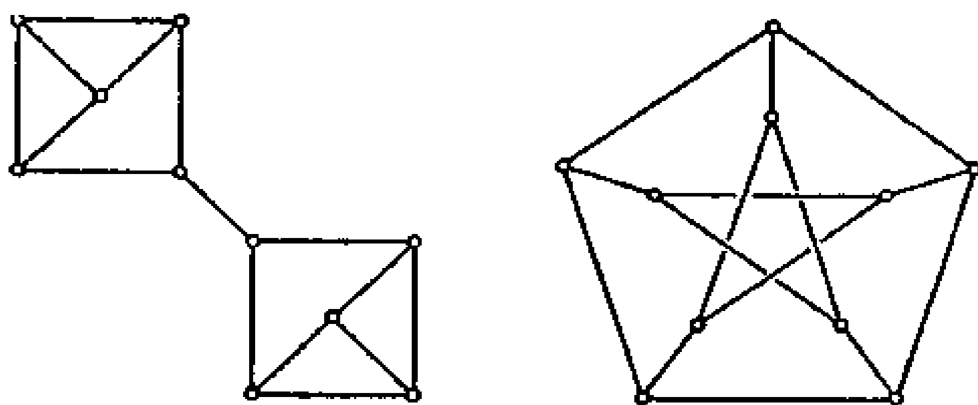
泰特相信,可用三种颜色将任一个三价图的边进行染色,使会于任一顶点的三条边的颜色各不相同.只要图是平面的且无桥,则此一论断就可能是对的.如果不加这些限制,论断就不成立了,看看下图就会了然,图中之一有一桥,另一个是非平面的.两个图都有 10 个顶点和 15 条边,但都不可能做到三染色.

---

① Proceedings of the Royal Society of Edingburgh, July 19, 1880, Vol. X, pp. 728—729; Philosophical Magazine, January 1884, series 5, Vol. XVII, p.41. 又见 Coxter, Journal of Recreational Mathematics, 1961. Vol. II, pp.3—12,或 Leonardo, 1971, Vol. IV, pp.273—277.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



[225] 图 8.2

彼得森(J. Peterson)①对其中的困难解释如下：他证明了任一个三价图可先用两种颜色染色，譬如说红色和绿色，使会于同一顶点的三条边之一为红色的，其余两条为绿色的.绿色的那些边构成一些环(多边形).显然，泰特假定了这种二染色可以如此配置，使每个多边形皆有偶数条边.这样一来，他就能将所有绿边交替地改染为蓝色的和黄色的了.

假定改进了的泰特猜想是可予以证明的，即，不具有桥的平面三价图是可以三染色的.他对于四色猜想的论证分为如下的两个部分.

首先，假定地图上任一点都不是多于三个区域的边界的汇合点.于是，全部边界可以看成是一个三价图，进而，据泰特的定理，这些边界可以用三种颜色 β, γ, δ 进行染色，而且在边界的任一汇合点处不会有两条颜色相同的边界相遇.假定已经做到了这一步.现在用四种颜色 A, B, C, D 来给地图上的各个区域染色.先给一个区域染成 A 色，再给以 β 为分界线而与 A 相邻

① 见 Julius Peterson (1839—1910), L'Intermédiaire des Mathématiciens, Vol. V, 1898, pp.225—227; Vol. VI, 1899, pp.36—38. 又见 Acta Mathematica, Stockholm, Vol. XV, 1891, pp.193—220.能够做到泰特要求的染色的最简非平面图有六个顶点：1,2,3,4,5,6 和九条边，每条边连接着一个奇数号的顶点和一个偶数号的顶点.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的区域染成 B 色，再给以 γ 为分界线而与 A 相邻的区域染成 C 色，再给以 δ 为分界线而与 A 相邻的区域染成 D 色. 照此进行下去，则 β 线的两侧总是 A，B 两种颜色或者是 C，D 两种颜色；γ 线的两侧总是 A，C 两种颜色或者是 B，D 两种颜色；δ 线的两侧总是 A，D 两种颜色或者 B，C 两种颜色. 容易看出，如果我们达到一个区域，它周围的区域都已经染上了颜色，那么越过任一条边界进入它时，按规则它所应该染上的颜色都是同一种颜色. 这也可由这样一个事实推出，即，如果我们把 β，γ，δ 看成是 [226]
一些算符，则 δ 可以等价地表示为 β 与 γ 按任一先后次序相继作用的结果. 于是，这类地图的染色问题已经解决.

其次，假定在某点处有四条或更多的边相会，于是图的价数大于 3. 在每一个此类点处都引入一个小区域如下，则问题化为第一种情况. 这样引入的小区域可以按前述规则染色；但当地图的其余部分都染完之后，这些小区域的任务就完成了，然后将它们都无限地缩小各成一个点，小区域都消失了而使边界都恢复成原先的样子.



图 8.3

化至标准图

为了进一步讨论这个问题①，需要建立将一个地图化至"标准"图的概念，它比原来的地图简单，而且如果简化图可以用四种颜色染成则原图也可以用四种颜色染成.（更不用说，如果简化图可以用五种或更多种颜色染成则原图也可以

① Heawood, Quaterly Journal of Mathematics, 1890, Vol. XXIV, p. 333. 他的这篇简述文章应归于帕尔斯(L. A. Pars).

我们必须知道，而且我们必将知道

那样.)

假定把地图画在球面上;它并未盖满整个球面,我们把"世界的其余部分"看成是又一个区域.其次,把顶点化为三价的,但不是用上述办法(因为那个办法增加了区域的个数)而是用另一种办法如下:注意到一个高价顶点周围至少必有一对不相邻的

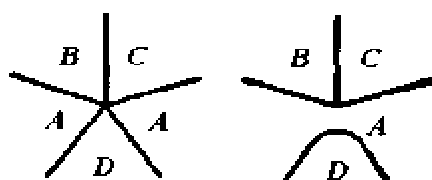


图 8.4

区域,可将它们染成同一种颜色;于是打开这个顶点并把这两个
[227] 区域合并成一个区域.第三步,清除那些仅有一条、两条或三条边的区域.(为此,只须去掉一条边而把此区域和一个相邻的区

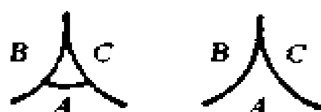


图 8.5

域合并.)第四步,清除那些具有四条边的区域.(围绕该区域的四个区域中至少有一对非相邻的区域;这一对区域就可以和这个四边形区域合并.如果这样得到的地图可以用四种颜色染成,

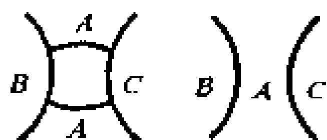


图 8.6

那么原来的地图也可以那样;因为当我们恢复所清除的四边形时,至多只有三种颜色围绕着它,我们还有可用于它的一种颜色.)第五步,清除所有的环形区域,从而所得每个区域皆由一条

我们必须知道，而且我们必将知道

http://maths352.bokee.com

连续曲线围成,而且任何一个区域都不包含另一个或多个别的区域.(一个环形区域可以用连接其内部与外部的走廊劈开,这内、外两个区域可以和走廊合并成一个区域.)

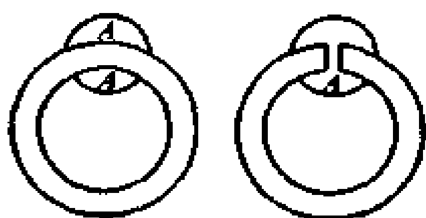


图 8.7

如果我们原先要染色的是一个颇为简单的地图,则如上约化的地图可能消失了,剩下的是覆盖整个球面的一个区域,对于此类地图来说,定理已被证明.最坏的情况下所剩的将是一个“标准”地图,它的任一个区域至少有五条边界.

这种地图可以看成是一个多面体,它有 F 个面(区域)、E 条棱(相邻区域的分界线)和 V 个顶点.自然可以把和 n 个区域相邻的区域称为一个 n 边形.于是,这 F 个区域包括 n 取各种 [228]
值的 n 边形.由于每个顶点属于三个区域,而每条棱属于两个区域,所以

$$3V=2E=\Sigma n,$$

这里 Σ 表示对于所有 F 个区域求和.据欧拉公式 $F-E+V=2$(我们将在本书第237—238页证明它)可知

$$\begin{aligned}\Sigma(6-n)&=6F-\Sigma n=6F-3\Sigma n+2\Sigma n\\&=6(F-E+V)=12.\end{aligned}$$

所以至少在一种情况下 $n<6$:至少有一个五边形.

现在我们可以用归纳法证明:一个标准地图,因而任一个地图,都可以用六种颜色染成.考虑一个五边形区域.将它和它的邻区之一间的边界线去掉而合并成一个区域.如果这新的地图可以用六种颜色染成,那么当我们恢复这个五边形区域时,它的周围至多只有五种颜色相邻,所以我们还有一种颜色可用以染它.然后,未染色的

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

区域可一步步减少.于是六色定理得证.(论证比乍一看来细微得多.因为,当去掉一条边后,新的地图不一定仍是"标准的"了.在再引用同样的论证之前,可能需要先用上述步骤之一去约化这个新地图.后边我将把这个程序称为"原始的归纳论法".)

据希伍德(P. J. Heawood)的一个更细致的论证①,我们还可以证明五种颜色总是够用的.考虑一个五边形区域 P.与它相邻的区域 Q,R,S,T,U 之中至少有一对彼此不相邻的,譬如说,Q 和 S.去掉 P 的两条边,使 Q,P,S 合并为一个区域 P'.如果所得的地图可以用五种颜色染成,那么原先的地图也可以;因为区域 P',R,T,U 至多用掉四种颜色,当恢复原先的地图时,还有一种颜色留给 P.再次一步步减少未染色的区域,直到五色定理得证.

可能失败的最小地区数

然而我们只能前进至此.除了对于较小的 F 值之外,五色
[229] 足够与四色(一般是)必要之间的间隙从未沟通.由于当 $n>5$ 时 $6-n$ 为零或负数,上述方程

$$\Sigma(6-n)=12$$

告诉我们每一个标准地图至少包括 12 个五边形.最简单的标准地图是二十面体.这种地图是可以用四种颜色染成的.由此可知每个不多于 12 个区域的地图都可以用四种颜色染成.换句话说,需要用五种颜色的地图必至少有 13 个区域,其中至少包括 12 个五边形.

这些数字已经被许多研究者改进了②.1922 年,富兰克林(P. Franklin)证明:一个地图如果必须五种颜色才能染成,那么

---

① 前注资料 337 页.

② Transactions of the American Mathematical Society, 1922, Vol. XLIV, pp.225—236; Annals of Mathematics, 1927, series 2, Vol. XXVIII, pp. 1—15; Bulletin of the American Mathematical Society, 1936, Vol. XLII, p. 491; Proc. London Mathematical Society, 1963, series 3, Vol. XIII, pp. 193—218.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

它必至少有 26 个区域. 1936 年他又把这个数字增加到 32,其中至少包括 15 个五边形. 不几年后,温(C. E. Winn)把这个数字增加到 36,其中至少要包括两个六边形区域.

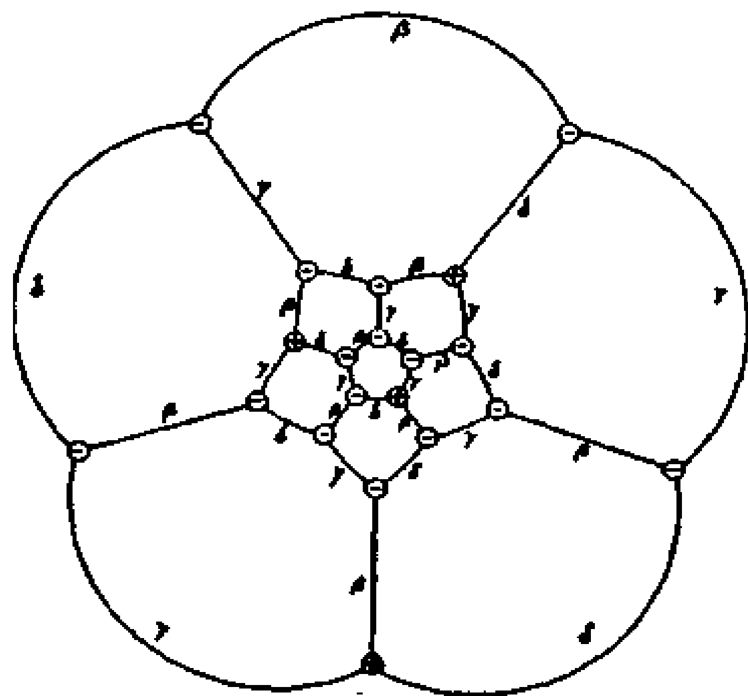


图 8.8

在希伍德的第二篇文章①里,他说明了怎样把问题化为纯数论的问题. 仍旧考虑泰特的三价图——$3n$ 条边连接着 $2n$ 个顶点(本书第 229 页). 在每个顶点有三条边相会,记为 β,γ,δ. 按照相会边 β,γ,δ 围绕顶点的顺序为逆时针的或顺时针的而把顶点分别为"正的"或"负的"两类. 于是每个区域有一些正的顶点和负的顶点,其个数相差一个 3 的倍数. 因为,沿顺时针方向依次看一个区域的各边时,每经过一个正的顶点时我们向前进一步,每经过一个负的顶点时我们向后退一步,这里进退指循环次序 β,γ,δ. 所以当我们回到出发的顶点时,向前转与向后转的步数之差必须是 3 的倍数. 反之,将顶点任意分成两类,则边总可以用 β,γ,δ [230]
分别标记. 于是泰特的论证就断定了此图可以用四种颜色染成.

① Quaterly Journal of Mathematics, 1897, Vol. XXIX, pp.277—278.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

等价的数论问题

把顶点分别为正、负两类和用取值为 +1 或 −1 的 $2n$ 个变数 $x_1, x_2, \cdots, x_{2n}$ 分派给它们. 于是染色问题就化为求解一组 $n+2(=F)$ 个形状为

$$x_a + x_b + \cdots \equiv 0 \pmod 3$$

的同余式的那种解组，其中任一个 x 皆不取零值. 这 $2n(=V)$ 个变数中的每一个皆恰好出现于这些同余式中的三个里. 于是，问题就是：是否每个这样的同余式组都有所要求的那种解.

再考虑形状为

$$x_a + x_b + \cdots \equiv \rho \pmod 3$$

的"推广的"同余式组，其中 ρ 可以取值 0, 1, 或 2. 希伍德发现①，当 n 增加时，"失败"(即，无解的同余式组)情况的数目迅
[231] 速递减. 可是在后来的一篇文章里他又证明了失败的情况(指推广的同余式组)总要发生.

无 边 曲 面

如果在某曲面的每一点处皆可适当指定一个正的旋转方向，则称此曲面为可定向的②. 通常空间里的一个曲面可否定向，视其为双侧的或单侧的而确定. 例如，本书第 130 页上所说的"立交环"可否定向即视 m 为偶数或奇数而确定.

为了研究一个无边曲面③(例如一个球的表面或者一个环

---

① Proceedings of the London Mathematical Society, 1932, series 2, Vol. XXXIII, pp. 253—286.

② 确切地说，任一点处的正旋转方向可用一个"准螺"定之，即，边沿上带有箭头的一个小圆. 如果在某曲面上可以找到一条闭曲线，当沿它走一圈时准螺反了向，则此曲面即为不可定向的.

③ 即，没有任何边界(即，边沿)的曲面. 关于有趣的无边曲面，参看 Steinhaus, Mathematical Snapshots, New York, 1938, pp. 117, 233, 237.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的表面)的拓扑性质，我们用一张地图把它整个盖住，即，将它划分为 F 个单连“区”，区的分界线共有 E 个弧，每个弧连接着一对顶点，顶点总共是 V 个．当曲面被挤压或拉伸时，地图也跟着变形，所以数字 F,E,V 不变．我来证明：数 $F-E+V$ 是曲面本身的一个性质而不是特殊某一张地图的性质，即，如果同一曲面上的另一张地图有 F' 个区域、E' 条边界线、V' 个顶点，则 $F'-E'+V'=F-E+V$．为此，假定把这两张地图重叠起来①，于是两组分界线可能彼此相交，从而构成第三张地图，不妨说它有 f 个区域、e 条分界线、v 个顶点．这第三张地图的 v 个顶点包括前两张地图的 $V+V'$ 个顶点②以及它们的分界线相交出的点．

让我们修正第一张地图，把刚才所说的交点也算做它的顶点，它们把自己所在的分界线一分为二．由于 E 与 V 同样多地
增加了，所以 $F-E+V$ 的值没有改变．现在可以把第三张地图 [232]
的分界线和顶点作为相接的“链条”添进去，每条链连接着两个顶点并且把它所在的区域一分为二．这样的链条由(不妨说) n 条线段组成，相会于 $n-1$ 个新的顶点($n\geqslant 1$)．这个链条把 F 增 1，E 增 n，V 增 $n-1$，所以 $F-E+V$ 不变．继续添链，直至完成第三张地图，于是我们发现 $f-e+v=F-E+V$．相仿地，$f-e+v=F'-E'+V'$．所以 $F'-E'+V'=F-E+V$．

不变量 $\chi=F-V+E$ 称为曲面的示性数③．通过考察曲面上一个简便的地图，就能找到该曲面的示性数．例如，对于一个

---

① 这个证法是亚历山大(J. W. Alexander)教授提醒我的．

② 这里假定了这 $V+V'$ 个顶点无有重合者，但无损于一般性，因为只要稍微将边界移动一些就可使重合的顶点分开．

③ 它在下述意义上“刻画”了曲面的特性：两个无边曲面，不论两者皆可定向或皆不可定向，只要示性数相同，就是同胚的(即拓扑等价的)．有些作者喜欢用与我们的 χ 反号的值，即，他们定义示性数为 $-V+E-F$．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

球面，可以利用四面体，此时 $F=V=4$ 而 $E=6$，故有结论 $\chi=2$. 从而证明了欧拉公式

$$F-E+V=2.$$

在本书第 137 页和第 233 页上都用过它.

由任一给定的曲面，可以通过增添一个“环柄”(handle)而导出和它拓扑不同的另一个曲面，所谓环柄，可以把它看成是一个弯曲的棱柱面，它连接着所给曲面上的地图中的两个相离的 n 边形. 这样的棱柱面有 $2n$ 个顶点(它们都在原给的曲面上)、$3n$ 条棱(其中除了 n 条之外都在原给的曲面上)、$n+2$ 个面(其中有两个面——底面——贴合在原给的曲面上，但它们已经被拿掉了). 所以，每增添一个环柄后，V 值未变，E 值增加了 n，F 值增加了 $n-2$，总之，示性数减 2.

最一般的(无边)可定向曲面可以看成是带有 p 个环柄的球面. 数 p 称为该曲面的亏格(genus). 于是，球面的亏格为零；环面的亏格为一. 上边的论述说明了示性数等于 $2-2p$. 所以任
[233] 一可定向曲面的示性数皆为偶数.

非定向曲面的示性数可以是偶数也可以是奇数(但不可能大于 1). 在通常的空间里，没有不自交的无边且不可定向的曲面.

对 偶 地 图

给定任一张地图(覆盖着一个无边曲面)时，可以定义一张对偶地图(覆盖着同一曲面)，它的每一个顶点位于原地图的一个相应的的区域内，并且它的每一条边界线和原地图的一条相应的边界线相交.(例如本书第 109 页上的那个例子.)显然，原地图的各个顶点分别位于对偶地图的不同区域内，而两张地图的关系是对等的. 对偶变换将数 F,E,V 依次变为 V,E,F. 一个“标准”地图的对偶地图里，所有的区域都是三角形的. 反多面体可以看成是对偶地图的一种特例.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

大十二面体$\left\{5,\frac{5}{2}\right\}$(本书第 153 页)是亏格为 4 的曲面上的一种地图,因为 $F-E+V=12-30+12=2-8$. 这种地图是自对偶的(或者说,和一个同样的地图成对偶),多面体$\left\{5,\frac{5}{2}\right\}$和$\left\{\frac{5}{2},5\right\}$是拓扑等价的(即"同胚的"). 在同样的意义上,多面体$\left\{3,\frac{5}{2}\right\}$和$\left\{\frac{5}{2},3\right\}$分别等价于通常的二十面体和十二面体.

四面体的旋转环(本书第 161 页)提供了环面上的由 $4n$ 个三角形构成的地图. 环面的亏格为 1,因为 $F-E+V=4n-6n+2n=0$.

各种曲面上的地图

最简单的不可定向曲面是射影平面,它可以看成是对极点(antipodes)被视为等同点的一个球面或者所有直径两端皆被视为等同点的一个圆盘. 这个曲面上最简单的地图就是画一条直径把它分成两个区域(二边形). 由于 $F=E=2$ 且 $V=1$,所以示性数 $\chi=1$. 下边更有趣的地图(其 $F=6, E=15, V=10$)是将正十二面体的对极点皆等同化而得到的. [234]

对于任一无边曲面上的标准地图,本书第 233 页上的论证说明

$$\Sigma(6-n)=6\chi.$$

正如当 $\chi=2$ 时一样,当 $\chi=1$ 时它也是正的. 因此,"原始的归纳法"既能证明球面上的每种地图皆可用六种颜色染成,它必也能证明射影平面上的每种地图也可用六种颜色染成. 图 8.9 中的"半十二面体"(它的六个面中每两个都相邻)提供了这样一个例子,它表明六种颜色是必要的;另一方面,如刚才所见,六种颜色也是足够的. 所以,逻辑上没有待补充的间隙. 射影平面的染色问题是完全解决了.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

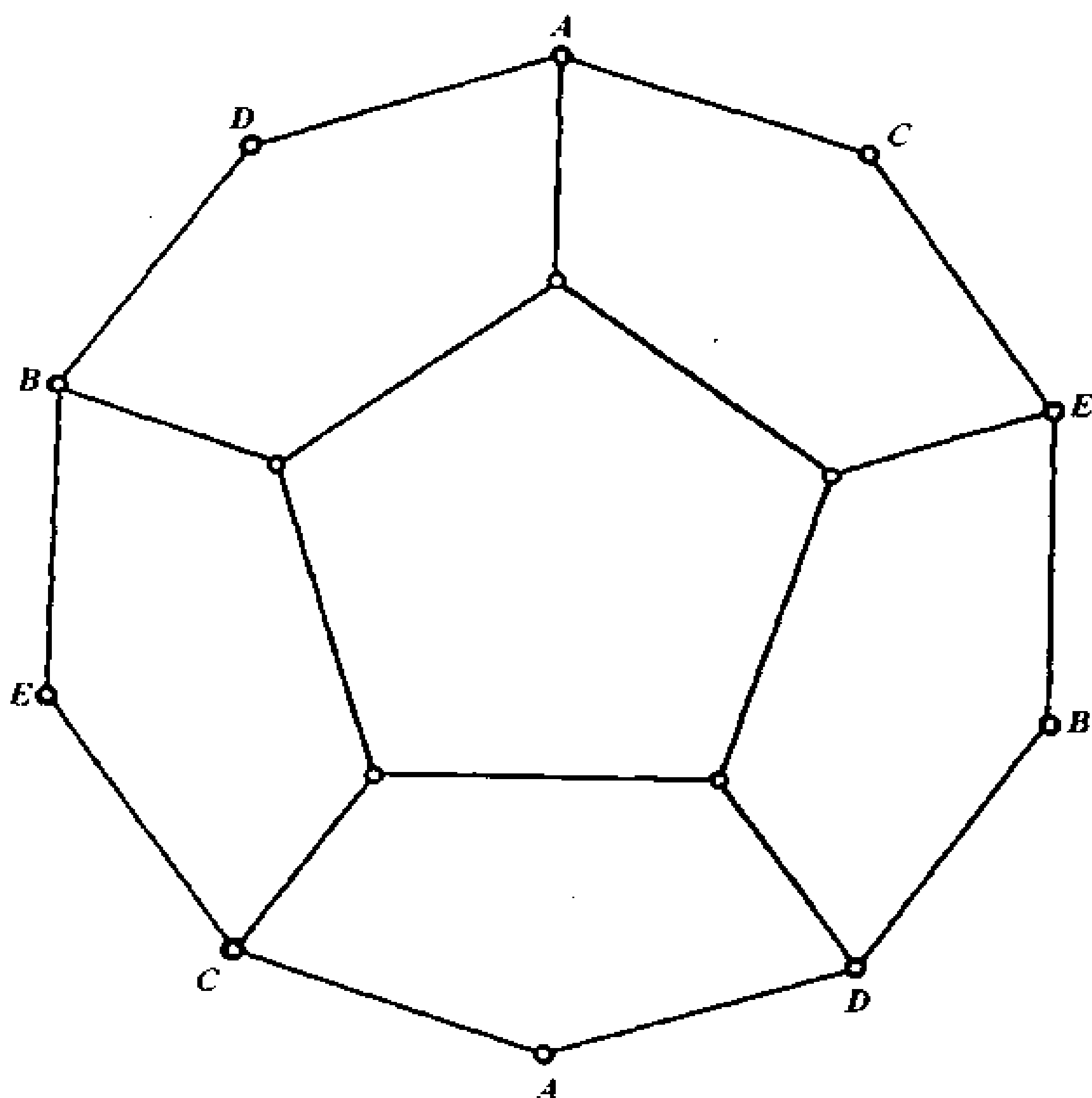


图 8.9

[235] 这是希伍德的“地图染色定理”(1890 年)的最简单的情况($\chi = 1$).此定理谓:为了给示性数 $\chi < 2$ 的无边曲面上的任一地图颜色,至多只需要$[N]$种不同的颜色,这里

$$N = \frac{1}{2}(7 + \sqrt{49 - 24\chi}),$$

$[N]$表示不超过 N 的最大整数.(他把 $-\chi$ 写成 k.)他的微妙而紧凑的论证可转述如下:

我们必须知道，而且我们必将知道

http://maths352.bokee.com

不必把地图“标准化”，需要的只是每个顶点都属于至少三个区域，于是

$$3V \leqslant 2E = \Sigma n.$$

由于 $\chi = F - E + V$，故 $E \leqslant 3(E - V) = 3(F - \chi)$. 再注意 N 是二次方程 $N^2 - 7N + 6\chi = 0$ 即

$$6(1 - \chi / N) = N - 1$$

的正根. 现在我们可以来证明下述引理：

在示性数 $\chi < 2$ 的曲面上的每种地图包含至少一个区域其邻区的个数少于 $[N]$. 即，至少有一个 n 边形，$n < [N]$.

当 $F \leqslant [N]$ 时这是显然的. 我们可以只考虑具有多于 $[N]$ 个区域的地图，故以下认为 $F > N$. 当 $\chi = 1$ 时，上边也证明过了. 现在假定 $\chi \leqslant 0$. 于是

$$\begin{aligned} \Sigma n = 2E &\leqslant 6(F - \chi) = 6(1 - \chi / F) F \\ &\leqslant 6(1 - \chi / N) F = (N - 1) F \\ &< [N] F. \end{aligned}$$

另一方面，如果每个 n 都大于或等于 $[N]$，则将会有 $\Sigma n \geqslant [N] F$. 于是，引理得证.

为了证明地图染色定理本身（它断言，若 $\chi < 2$，则 $[N]$ 种颜色总是足够的），我们作一个归纳假设：它对于每个只有 [236]
$F - 1$ 个区域的地图成立. 然后考虑一个给定的有 F 个区域的地图，特别注意一个少于 $[N]$ 个邻区的区域. 将此给定的地图作一修改，使这个区域缩为一个点. 于是我们得到一个新的地图，它只有 $F - 1$ 个区域，从而可用 $[N]$ 种颜色染成. 假定这样做了，并用同样的染色安排去染原给的地图，即，涂染其除了上述一个特别的区域之外的一切其他区域. 那么，即使其所有邻区的颜色皆不相同，它们也只用了至多 $[N] - 1$ 种颜色，所以尚有第 $[N]$ 种颜色可用以染这个特别区域. 由于这个论证当 $F = [N] + 1$ 时成立，所以当 $[F] = [N] + 2$ 时也成立，依次类推，$[N]$ 色染色定理从而对一切 F 值皆

我们必须知道，而且我们必将知道

成立.

例如,在环面(它是一个 $\chi=0$ 的可定向曲面)上很容易画出由七个彼此相邻的六边形构成的一个七色地图.

在本书第 132 页上我们曾提到过叫做麦比乌斯带的有趣的曲面.这是一个有边曲面,它的边缘是一个单环道,即,一个拓扑圆,正如一个盘子的边缘一样.理论上(虽然不是在通常的空间里!),在这个边缘线上嵌入一个盘面,我们就得到一个无边曲面.不难看出,这样得到的无边曲面就是一个射影平面①,其 $\chi=1$.另一个可能的做法是把两个麦比乌斯带沿着它们的公共边缘黏合起来,这样得到的无边曲面就是所谓的克莱茵瓶②,它是一个 $\chi=0$ 的不可定向曲面.由于这个曲面与环面有同样的示性数,希伍德的定理告诉我们,它的地图至多只需要七种颜色.在这种简单情况下,我们能够更前进一步:富兰克林证明了③克莱茵瓶上的每个地图都可用六种颜色染成.这是希伍德数[N]
[237] 并非充要的唯一情况.格哈特·林格尔(Gerhard Ringel)与扬斯(J. W. T. Youngs)④做了大量的工作终于证明了:除克莱茵瓶外,每个无边曲面上都可以画出一个由[N]个彼此相邻的区域构成的地图.

谷底,峰顶,鞍点

回到球面(它的 $\chi=2, N=4$)的情况,我扼要地谈谈欧拉公

---

① 例如,见于 Coxter, Introduction to Geometry, p.383.

② D. Hilbert and S. Cohn-Vossen, Geometry and the Imagination, New York, 1952.

③ Journal of Mathematics and Physics, 1934, Vol. Ⅻ, pp.363—369.(这是一篇特别有趣的文章.)

④ Proceedings of the National Academy of Sciences, U.S.A., 1968, Vol. LX, pp.438—445.

http://maths352.bokee.com

式在一个地文问题[1]上的应用，这问题是关于一个干燥行星上的谷底、峰顶与鞍点数目之间的关系问题. 一个峰顶就是一个局部最高点，一个谷底就是一个局部最低点. 每个峰顶或谷底都被一族等高线围绕着. 一个鞍点就是一条等高线的自交点. 等分由等高线自交所成的角，在每个鞍点处得到四个方向. 如果由鞍点出发沿着它们之中的任一方向前进，那么人们将沿着最大陡度线——或者说分水岭而上到一个峰顶，或者沿溪床而下到一个谷底. 显然，峰顶与反向的分水岭偶可以被看成是一个地图的顶点与分区线，它的每个区域(谷)内有一个谷底. 所以，如果有 F 个谷底、E 个鞍点、V 个峰顶，则

$$F - E + V = 2.$$

相仿地，谷底与反向的溪床偶是对偶地图的顶点与边界线，它的每个区域(山)里有一个峰顶.

正二十面体的染色

一个四面体的表面作为地图可以用四种颜色按四种方式染成，一个正十二面体的表面[2]则可按四种方式染成，这四种方式构成两对配偶. 一个正八面体或一个立方体的表面分别可以用 [238]
两种或三种颜色染成，但皆只有一种方式. 那么，有趣的是一个正二十面体竟可用三种颜色按 144 种之多的方式染成. 这个数目似乎是首先被安德烈斯得出的.

不难发现，要把正二十面体进行染色而不许和任一面相邻

---

[1] A. Cayley and J. Clerk Maxwell, Philosophical Magazine, 1859, series 4, Vol. XVIII, pp.264—268, and 1870, series 4, Vol. XL, pp.421—427. 又见 D. A. Moran, American Mathematical Monthly, 1970, Vol. LXXVII, p.1096.

[2] 见史泰因豪斯(H. Steinhaus)的 Mathematical Snapshots 末尾所载优美的自展模型.

我们必须知道，而且我们必将知道

[redacted]

的三个面的颜色皆相同是办不到的.事实上,总有两个那样的面.假定所用的三种颜色是白、黑、灰,并假定黑面之一被三个白面围绕着,其中每两个白面之间夹着另外两个面,它们必须是一黑一灰(因为二者相邻).再往外去还有和它们相邻的两个面,这后两个面的颜色必须是灰与黑、白与黑、灰与白或者两者皆为白色.用 a,b,c,d 分别记这四种可能,并视当我们绕着原先的黑面进行时首先说的"一黑一灰"发生的顺序是顺时针方向或逆时针方向而确定要不要在这些字母上添一个小撇.现在可以用 a,b,c,d 中的三个字母(允许重复,必要时适当带撇)来表示染色(20 个面中的 $1+3+6+6$ 个)的方案.轮换三个字母时.染色方案实际并未改变,自然要用同样的符号去表示轮换这些颜色所得的染色方案.在对 a,b,c,d 所指定的上述含义中,黑色只是表示所说的特殊面的颜色,白色只是表示与特殊面相邻的三个面的颜色,灰色只是表示第三种颜色.

给定任一个染色方案之后,将特殊面的黑色改为灰色,我们就得出另一个染色方案.它与保留特殊面的黑色而交换其他黑面与灰面的颜色是等价的,这包括着 b 换为 c,c 换为 b,并添加或去掉小撇.(如 a^2b 变成 a'^2c'.)

在上述十二个情况里,前 16 个面的染色完全确定了其余四个面的颜色.(在图 8.10 中,二十面体被沿着外接球面半径的方向射影到球面上,然后再经球极平面射影到一个平面上.顶点之一被投射到无限远.在每种情况里,特殊的黑面都是正好在图形
[239] 中心正上方的那个面.)

我已经说过,总有第二个面,它的三个邻面的颜色也是全都相同的.(在图 8.10 中,这个面都用一个点示明.)适当调换颜色,这个面总可成为一个被三个白面包围着的黑面,然后可指派给它另一个符号,用以表明在第二种观点下的染色.这种外貌上的改变不会改变 $a^2b, ab^2, adc, b'c^2$,但把 $ac^2, b^2c', ad'b', adb'$ 分别与 $a'd'b', ac'd', ac'd, ad'c$ 相交换.由于两个特殊面中哪

我们必须知道,而且我们必将知道

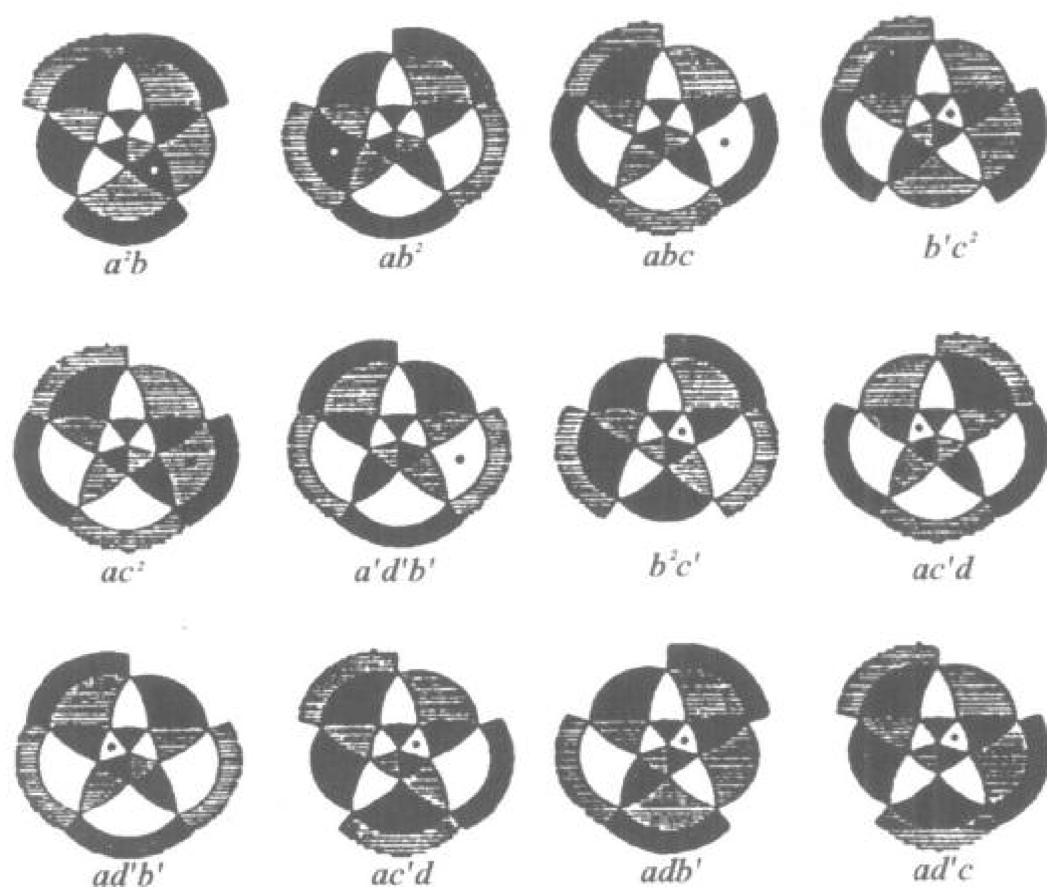


图 8.10

个也不比另一个更优先，所以还是把相应的两个符号合并起来好，这样就把各种染色方案记为$(a^2b)^2$，$(ab^2)^2$，$(adc)^2$，$(b'c^2)^2$，$(ac^2)(a'd'b')$，$(b^2c')(ac'd')$，$(ad'b')(ac'd)$，$(adb')(ad'c)$.

经过镜面反射，这八种染色方案各自又产生另一种方案.新方案的符号可由增减小撇并反转每组中三个字母的轮转次序而得之.例如由$(b^2c)(ac'd')$导出配偶$(b'^2c)(a'dc)$. [240]

在图 8.11 所示的九种情况里，前 16 个面的染色不能确定其余四个面的颜色.不过，利用双重符号可以消除其不确定性.

为了说明它们和它们的配偶概括了一切可能的方案，我只须将一切三字母的轮换小组列成一个表，并把其中包含下列两两相继字母的小组删掉：aa'，$a'a$，ab'，ba'，$a'c$，$c'a$，bb'，$b'b$，

我们必须知道，而且我们必将知道

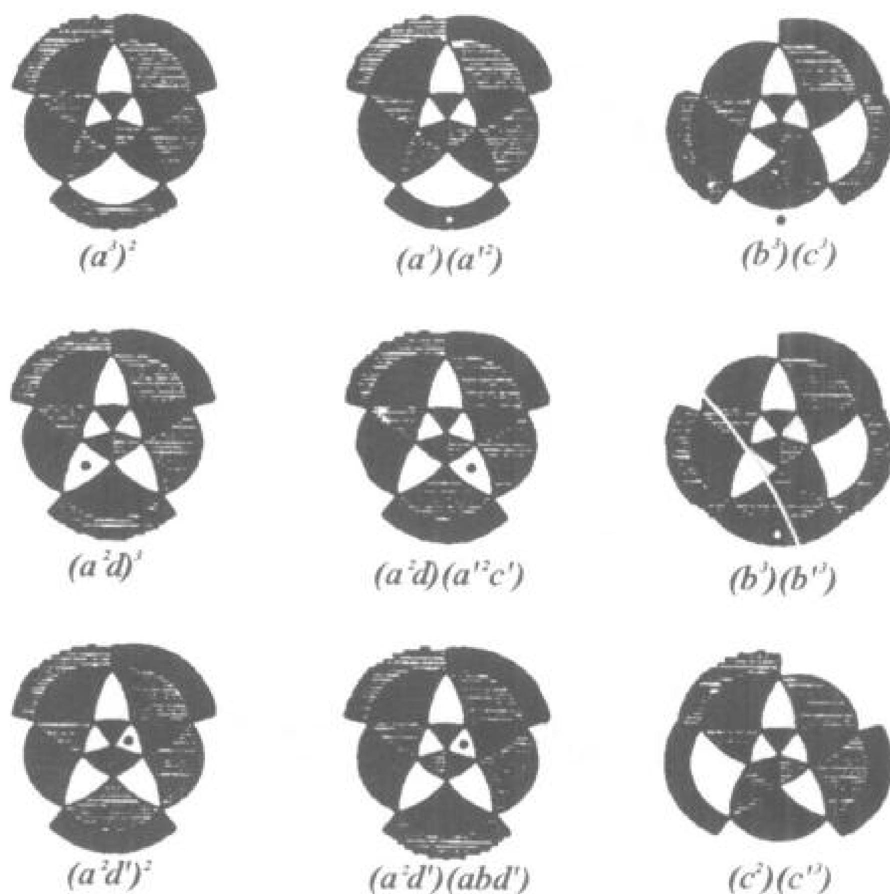


图 8.11

cc', $c'c$, bc, $c'b'$, $b'c'$, cb, $b'd$, $d'b$, $b'd'$, db, cd, $d'c'$, cd', dc', d^2, dd', $d'd$, d'^2. 这是因为每两个这样的相邻字母都导致颜色相同的两个面. 同样的理由也要求删掉三字母组 acb' 与 $a'bc'$. 剩下的三字母组恰好是上边所说的那些方案.

现在进行具体的枚举如下: 14 种染色方案 $(a^3)^2$, $(a'^3)^2$, $(a^2b)^2$, $(a'^2b')^2$, $(ab^2)^2$, $(a'b'^2)^2$, $(a^2d)^2$, $(a'^2d')^2$, $(adc)^2$, $(a'c'd')^2$, $(a^2d')^2$, $(a'^2d)^2$, $(b'c^2)^2$, $(bc'^2)^2$ 中任一对当交换某
[241] 两种颜色时都不变; 所以它们(轮换其颜色)给出 42 种方案. 对于方案 $(b^3)(b'^3)$ 来说, 交换两种颜色和镜面反射是等价的; 这样又得到 12 种方案. 最后, 还有 15 种染色方案: $(a^3)(a'^3)$, $(b^3)(c^3)$, $(b'^3)(c'^3)$, $(a^2d)(a'^2c')$, $(a'^2d')(a^2c)$, $(ac^2)(a'd'b')$, $(a'c'^2)(abd)$, $(a^2d')(abd')$, $(a'^2d)(a'db')$, (b^2c')

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$(ac'd')$，$(b'^2c)(a'dc)$，$(ad'b')(ac'd)$，$(a'bd)(a'd'c)$，$(adb')(ad'c)$，$(a'bd')(a'c'd)$. 它们都可以作六种置换颜色，所以给出 90 种方案，从而共有 $42+12+90=144$ 种方案.

六个方案 $(a^3)(a'^3)$ 都有一个特点，即，在镜面反射后方案不改变. 可以称这六个方案为自反方案，而其他 138 个方案构成 69 个配对.

塔克曼(L. B. Tuckerman)说，可以用五种颜色去给一个正二十面体的面染色而使每个面和它的三个邻面四者的颜色皆不相同. 五种颜色给定时，这样的染色可以有四种不同的方案，它们构成两两配对，其中一对可以从另一对经过五种颜色的任一种奇置换(例如，交换两种颜色)而得到. 颜色相同的面分别属于本书 141 页上所说的穿叉成这个复合体的五个正四面体的表面.(参看 Coxeter, Regular Polytopes, pp.50,106.) [242]

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第9章 单行线问题

在这一章里我打算介绍几个来自单行线理论的几个问题.从欧拉的问题与定理开始,并将其结论简单地应用于迷宫与几何树.在本章末尾将讨论哈密顿游戏的逆单行线问题.

欧拉的问题

欧拉的问题最早出现于他在1736年提交给圣彼得堡科学院的一篇学术报告里①,在那篇报告里他解决了当时正在讨论中的一个问题,该问题即:从王堡镇的任一点出发去散步,问是否可能过遍所有的桥且每座桥只过一次而回到出发点?

此镇建于普雷格尔(Pregel)河口附近,其水路如图9.1所示,河中有一个克乃普豪夫(Kneiphof)岛.18世纪中,那里有七座桥,其位置如图所示.容易看出,在那种布局下,问题的答案是"不可能"(后来,又建了两座桥).不过,欧拉的研究并不限于王堡的特定情况,他讨论了任意几个岛被任意几座桥以任意的方式连通起来的一般问题.显然,如果我们把岛分别都缩小成一个点,并且把
[243] 桥分别代之以线,则问题的性质不会改变.这样我们终于得到一

① "Solutio problematis ad Geometriam situs pertinentis", Commentarii Academiae Scientiarum Petropolitanae for 1736, Leningrad, 1741, Vol. Ⅷ, pp.128—140.此文已由亨利(M.Ch.Henry)译成法文;见 Lucas, Vol. Ⅰ, part 2, pp. 21—33.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

个几何图，或者说，一个网络．在王堡问题中，这个网络如图 9.2 所示．点 A，B，C，D 表示地区，线 l，m，n，p，q，r，s 表示桥．

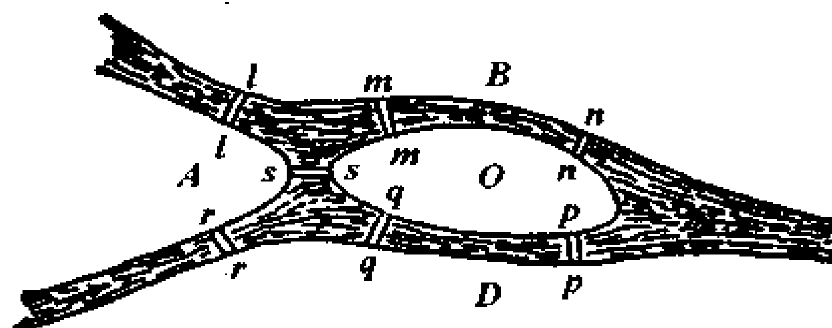


图 9.1

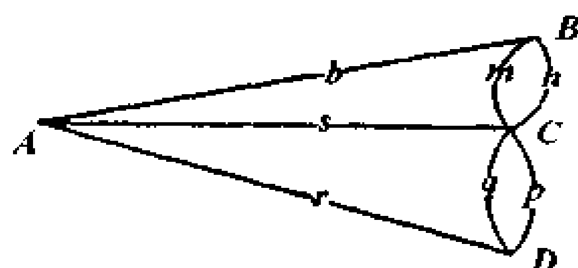


图 9.2

于是，欧拉的问题就是要判定一个几何图是否可以一笔画成．所谓一笔画就是不许笔离开纸面且每条曲线只许描绘一遍．更一般的问题是要求确定最少须几笔才能画成，笔一离纸就算一笔，每条曲线仍只许描绘一遍．这些都概括在后边所给的法则里．图可以是平面上的，也可以是空间里的．线可以是直的、也可以是弯的或扭曲的，它们连接着一些点．可以用一些两头带钩的细棒或线绳制作成图的模形，钩子是为了可以将它们随便几根连结于一点．

此种图的理论被包括在利斯丁的拓扑学①中的一些命题里

① Göttinger Studien, 1847, part Ⅹ．也可参看泰特的文章“Listing's Topologie”，载于 Philosophical Magazine, London, Jan. 1884, series 5, Vol. XVII, pp.30—46；或 Collected Scientific papers, Cambridge, Vol. Ⅱ, 1900, pp.85—98．威尔逊(J. C. Wilson)在他的 *Traversing of Geometrical Figures* (Oxford, 1905)里对此问题有所论述．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

[244] 而为其特殊情况.不过我在这里将采用欧拉的方法,并且为了论述简明,将先给出几个定义.

线的起点或终点称为*节点*(或岛).连接相继两个节点的线称为*支路*(或桥,或通道).会合在一个节点的支路数目称为该节点的阶.只有一条支路到达或出发的节点称为悬浮节点或悬浮端点,支路的每个终止点称为*端点*(或钩子).如果在某节点有偶数条支路相会,则称之为*偶节点*.显然,二阶节点的出现是无关紧要的.如果在某节点有奇数条支路相会,则称之为*奇节点*.没有自由端点的图是闭合的,此种图常称之为一个*闭网络*.

一条*路线*包括一些先后相继的支路,并且任一支路不得行经两次.终点与起点重合的道路称为*闭路*(或环).如果整个图构成一条路线,则称之为*一笔画成的*.

下边是欧拉的结论:(i)在任一网络中,奇节点的个数必为偶数.(ii)一个没有奇节点的图必可一笔画成,并且它还是一条闭路,从而它的任一点都可以作为起点.(iii)一个有且仅有两个奇节点的图可以一笔画成,画时从一个奇节点开始而终止于另一个奇节点.(iv)一个具有多于两个奇节点的图不能一笔画成;对此,里斯丁给出推论说,如果一个图恰有 $2n$ 个奇节点,则必可用 n 笔画成.

现在我来证明这些论断.

1. *网络中奇节点的个数必为偶数.*

假设支路的条数为 b.于是钩子的数目为 $2b$.令 k_n 表示 n 阶节点的个数.因在一个 n 阶节点有 n 条支路相会,故那里有 n

[245] 个钩子.

$$\therefore \quad k_1+2k_2+3k_3+4k_4+\cdots+nk_n+\cdots=2b.$$

于是 $k_1+3k_3+5k_5+\cdots$ 为偶数.

$$\therefore \quad k_1+k_3+k_5+\cdots \quad 为偶数.$$

2. *一个没有奇节点的图必可一笔画成,并且它还是一条闭路.*

我们必须知道，而且我们必将知道

http://maths352.bokee.com

路线显然是闭合的，所以不论从哪里开始都一样.假定从节点 A 开始.每当我们通过一个节点时，必然要在到达它时经过一个钩子而离开它时又经过一个钩子.因为没有奇节点，所以每个节点处的钩子数都是偶数.因此当我们到达 A 以外的其他节点时，总可以找到一个钩子，它把我们引到一条没有走过的支路.于是路线最终必把我们引到出发的节点 A.如果在 A 点有多于两个钩子，那么我们可以再沿着一条尚未走过的支路离开 A，但是和前一次一样我们最终仍将回到 A.

剩下还须证明我们能够安排我们的路线使它包括所有的支路.假定我们的图的每条支路都换成一条两端各带一钩的绳子，并且每个节点处的钩子都钩在节点上.每个节点处的钩子数都是偶数.假定把钩子都从一个节点上摘下来并且任意地两两钩到一起，每个节点处都这样做.于是整个模型构成一个或几个闭曲线，因为现在每个新的节点都只有两个钩子钩在一起.

如果这样随机地两两相钩的结果是一条曲线，那么定理已被证明，因为从任一点开始，我们都将经过每条支路而回到原处.如果这样随机地两两相钩的结果有一个孤立的闭路 L，它在结点 P 处与另一闭路 M 相触，那么把这个节点 P 处的四个(闭路 L 的两个和 M 的两个)钩子都脱开，然后重新把它们任意配合[①]再钩起来.于是 L 成为闭路 M 的一个部分.对于每个分离的回路都这样重新钩连起来，我们就逐步把所有的分离的闭路都变成同一个闭路的各个阶段了. [246]

例如，假定有三个岛，A，B，C，两两之间都有两座桥相连.在端点 A，B，C 的最不利的两两耦合是使 ABA，ACA，BCB 各自都成为一个闭路.闭路 ABA 与 ACA 在 A 相触.所以我们要重新搭配挂在 A 点上的钩子而把 ABA 和 ACA 合并成一个闭路

① 当然不要又搭配成原先的样子.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

ABACA.相仿地,重新搭配挂在 *B* 点上的钩子,把闭路 *BCB* 与 *ABACA* 合并.于是全部支路构成一个闭路.

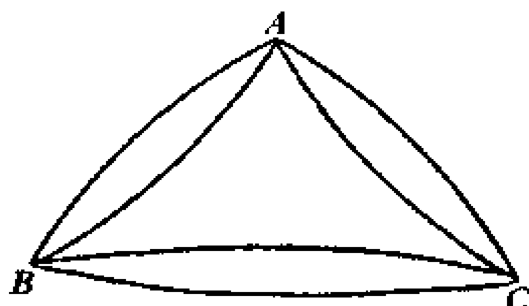


图 9.3

我据欧拉的话推度他曾经试图给出一个实用的法则,不必看到图的形状,按照法则就能一笔把它画出来.然而他未能成功.不过,他还说过:如果几何图的每条线都要求描画两次,那么任一几何图都可以一笔画出来,因为假定每条支路都是双重的,那么就没有奇节点,因而是可以一笔画成的.在这种情况下,任一图都可完全画出来而无须看到它的形状.下边将给出这种法则.

3. *如果一个图有且仅有两个奇节点,那么必可一笔将它画成,画时从奇节点之一出发而终止于另一奇节点.*

这个定理可以马上归结于第二个定理.设 *A* 和 *Z* 是两个奇节点.增添一条由 *A* 到 *Z* 的支路.考虑这个新图.这时所有的节
[247] 点都是偶节点了.于是,据第二个定理,可以将它一笔画成.不妨以 *Z* 为起点,那么 *Z* 也是终点.可以认为 *ZA* 是第一条支路.去掉这条支路,图就恢复成原先的图.于是 *A* 就成为起点而终点仍是 *Z*.

4. *若一个图恰有 $2n$ 个奇节点,则必可用 n 笔将它完全画成.*

如果任一条路线从一个奇节点开始,并且继续走下去直至到达一个节点,那里已经没有新的支路可走,那么这后一个节点

我们必须知道，而且我们必将知道

http://maths352.bokee.com

必是奇节点.因为每当到达一个偶节点时,必有一条可以离开它的支路。相仿地,每当我们通过一个奇节点时,必在到达时经过一个钩子而离开时又经过一个钩子.但是当它是一条路线的终点时,我们只到达该点,故只经过一个钩子.如果把这条路线抹掉,那么剩下的图将只有 $2n-2$ 个奇节点.因此,抹掉 n 个这样的路线之后,剩下的将是一个或多个仅有偶节点的网络.但是它们中的每一个必有几个与已抹去的路线共有的节点,因而皆可作为那些路线之一的一部分.所以整个通道恰有 n 条而不多于 n 条路线.由此得知,正如欧拉说过的,如果有多于两个的奇节点,则该图不可能一笔画成.

王堡的桥构成一个具有四个奇节点的网络,因此,据欧拉的第四定理,如果每座桥只许走过一次,则在一趟散步中不可能走遍,但是可以在两次散步中走遍.

图 9.4 中左图与中图都只含偶节点,所以它们都可以一笔画成.左图是一个五芒星 $\left\{\frac{5}{2}\right\}$(见本书 150 页 ~ 151 页);中图是所谓穆罕默德(Mohammed)签署,据说最初是他用刀尖在沙地上一刀画出来的(刀尖不离地面,画过的任何部分都不再重复).它只含偶节点,所以一刀画出是可以的.图 9.4 中的右图取自泰特的文章,它含有两个奇节点,所以也可以一笔画成,画时须从奇节点之一出发而终止于另一个奇节点. [248]

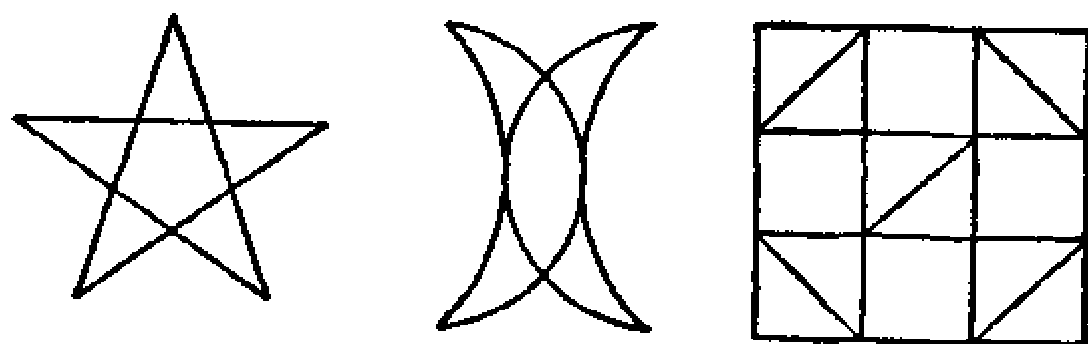


图 9.4

我们必须知道,而且我们必将知道

http://maths352.bokee.com

多边形$\left\{\frac{5}{2}\right\}$,即所谓三重三角形或五芒星,曾被毕达哥拉斯学派用以作为表记,彼此相互识认.这个符号也被认为是健康的标志,有时还在它的五个角上写上希腊字 ὑγίεια 的字母,用 θ 代替其中的双辅音 ει.这方面的权威伊安布里霍斯(Iamblichus)讲过这样一个故事:

一位毕达哥拉斯学派的学者在旅途中病倒在路边一家小客栈里,贫病交加,一筹莫展.店主甚宽厚,慷慨招待,悉心护理.虽经百般医治,然而此生病情却日渐恶化,自料即将绝命,无以报答店主.他要了一块木牌,画上一个五芒星,请店主挂到门外,告以如此则他的仁慈必得到报还.学者死后,主人妥为安葬,并依嘱将木牌一直悬挂着.久后,某日有旅客骑马经店前过者,见此庄重的标帜,解鞍询之主人.主人俱以告.旅者闻悉,乃厚酬之.

这虽是一则轶事,即便查无实据,编得也颇为圆满.

作为另一个一笔画的例子,是将一个$(2n+1)$边形的每个顶点都和其他的顶点连以直线所得的图.正八面体的所有的棱也构成一个一笔画.另一方面,通常用直线分成 64 个方格的棋
[249] 盘有 28 个奇节点,所以要用 14 笔才能画出所有的路线而不重复其任一段.还有,本书第 177 页上的图有 20 个奇节点,所以需要 10 笔才能画成.

一笔画法的个数

以下转来讨论:当一个图的节点都是偶节点时,可以有多少不同的方式将它一笔画成?①

让我们首先考查一条从 $2n$ 阶节点 A 出发并回到 A 的闭路 L 对问题的影响.如果把这条闭路抹掉,所剩图的节点仍然都是

① 参看 G. Tarry, Association Française sur l'Avancement des Sciences, 1886, pp.49—53.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

偶的，而 A 这时降为 $2(n-1)$ 阶节点. 假定原图有 N 种画法，新图有 N' 种画法. 那么这 N' 条路线中的每一条都通过 A 点 $(n-1)$ 次，而且每次通过都可按 L 的两种相反方向之一进行. 所以 $N=2(n-1)N'$.

相仿地，如果原图中的节点 A 是 $2(n+l)$ 阶的，并且有 l 条独立的闭路始于 A 而终于 A，那么就会得到

$$N=2^l n(n+1)(n+2)\cdots(n+l-1)N',$$

这里 N' 是抹掉这 l 条闭路后所得图的可能描绘方式的个数.

利用这些结论，我们可以把任何一笔可画成的图简化为不具有上述那种闭路的图. 假定这个简化图有 k 个节点. 如果用两个或多个分离的图（它们之中每一个的节点至多只有 $k-1$ 个）代替这个简化图，那么我们还可以抹掉这些节点之一，譬如说，A. 因为，假定节点 A 的阶数是 $2n$. 那么会于 A 的 $2n$ 条支路可以有 $1\cdot3\cdot5\cdot\cdots\cdot(2n-1)$ 种方式的配对，而每种配对都将构成一种通过 A 的通路，或者（在一对中的两条支路都连到另一个节点 B 的特殊情况下）构成一个环. 这条通路或环将构成通过 A 的路线的一部分. 所以原图的可能描 [250]
绘方式的个数等于这 $1\cdot3\cdot5\cdot\cdots\cdot(2n-1)$ 个较简单的图的可能描绘方式的个数之和.

将会看出，解决问题的步骤就是逐步把节点一个个抹掉. 采取这种步骤继续进行下去，我们最终将把图简化为无闭路的图，而且在每个这样的图中只有两个节点. 如果这些图中的任一个里的每个节点都是 $2n$ 阶的，容易看出它可以有 $2\cdot(2n-1)!$ 种画法.

我们知道：一个仅有两个奇节点 A，B 的图是可以一笔画成的，始于 A 则终于 B、始于 B 则终于 A. 所以一笔画成它的画法的数目就是连接 A 与 B 而成此图的连接法的数目. 因为若从 A 开始，在构成此图的任一路线的端点 B 我们显然可以沿 BA 而达于出发的节点 A.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

这个理论曾被塔里先生用于确定张数为偶数的一副骨牌可以连排的数目①.

一副普通的 28 张骨牌上的符号是:

6－6, 6－5, 6－4, 6－3, 6－2, 6－1, 6－0,
5－5, 5－4, 5－3, 5－2, 5－1, 5－0, 4－4,
4－3, 4－2, 4－1, 4－0, 3－3, 3－2, 3－1,
3－0, 2－2, 2－1, 2－0, 1－1, 1－0, 0－0.

在许多游戏中都用到骨牌. 除了例外, 在大多数情况下的玩法都是要求把牌排列成行使相继牌的相邻正方形上的符号相同. 譬如, 桌上放了一张 6－3, 则可以靠 6 那一端接放的牌只有 6－6, 6－5, 6－4, 6－2, 6－1 或 6－0. 相仿地, 靠 3 那一端只能接放 3－5, 3－4, 3－3, 3－2, 3－1 或 3－0. 假定把对子牌②放到适当
[251] 的位置上, 那么容易看出一副骨牌将形成一条闭路③. 我们要确定此种可能的行或闭路的数目.

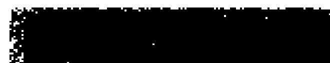
让我们先考虑一副最大点数达到双四的 15 张骨牌. 这 15 张牌中有 5 张是对子牌. 其余 10 张可以用一个正五边形的边和对角线代表之, 如 01, 02 等等. 对角线的交点不参与表示, 故可予忽略. 于是由边和对角线构成的图共有五个偶节点, 因而是可以一笔画成的. 任一一笔画的路线 (如 0－1, 1－3, 3－0, 0－2, 2－3, 3－4, 4－1, 1－2, 2－4, 4－0) 皆给出这 10 张牌的排列方式. 假定有 a 条这样的路线. 在每条这样的路线中我们可以把 5 张对子牌分别添进两个可能的位置之一里 (例如, 在上边给出的路线中, 可以把双二放入 0－2 与 2－3 之间, 或 1－2 与 2－4 之

① 参看本书法文本第 2 版, Paris, 1908, Vol. Ⅱ, pp. 253—263; 或看 Luas, Vol. Ⅳ, pp. 145—150.

② 即 6－6, 5－5, 4－4, 3－3, 2－2, 1－1 或 0－0. ——译者注

③ 因此, 如果拿掉一张 5－4, 则余牌所成的行必然一端止于一个 5 而另一端止于一个 4.

我们必须知道，而且我们必将知道



间）. 所以，15 张牌的一笔画的排列的总数是 2^5a. 如果我们把这些牌排成一条直线，则由于可以把 15 张中任一张作为开头的一张，所以总的排列数是 $15\cdot2^5\cdot a$.

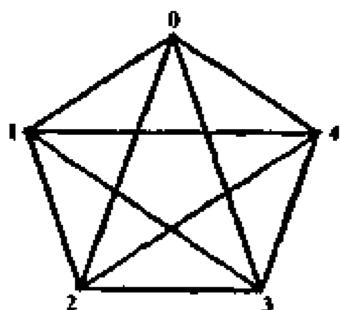


图 9.5

其次我们须求出图9.5中所画的五边形的一笔画路线的数目. 在节点0处有四条通路，它们可以有三种配对法. 如果0－1与0－2配成一对，0－3与0－4配成一对，则得到图9.6. 如果0－1与0－3配成一对，0－2与0－4配成一对，则得到图9.7. 如果0－1与0－4配成一对，0－2与0－3配成一对，则得到图9.8. 令 b 表示图9.6的画法数目，c 表示图9.7的画法数目，d 表示图9.8的画法数 [252]
目. 在图9.5中的五边形里抹掉节点0的效果是给我们留下图9.6～图9.8这三种四边形. 按上述记号，得到 $a=b+c+d$.



图 9.6

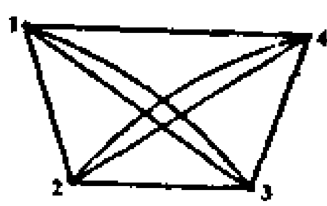


图 9.7

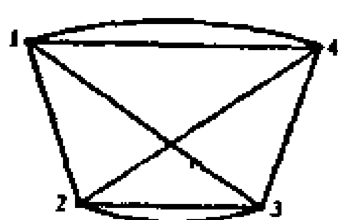


图 9.8

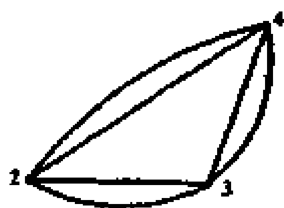


图 9.9

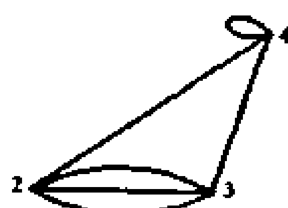


图 9.10

我们必须知道，而且我们必将知道

http://maths352.bokee.com

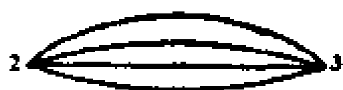


图 9.11



图 9.12



图 9.13

取这些四边形中的任一个，例如图 9.8 中的四边形．我们可以把会于节点 1 的支路两两耦合到一起而抹掉节点 1．如果把 12 与 14 的上条路耦合，13 与 14 的下条路耦合，就得到图 9.9．如果把 12 与 14 的上条路耦合．13 与 14 的下条路耦合，仍然得到图 9.9．如果把 12 与 13 耦合，14 的上下两条路耦合，则得到图 9.10．于是①和上边一样有 $d=2e+f$．相仿地，$b=2e+f$，$c=2e+f$．所以 $a=b+d+e=6e+3f$．

往下再考虑简化的图9.9和9.10．先拿图9.9来看，我们要抹掉其中的节点4．为行文简明计，用 β 和 β' 记42的两条支路，并用 γ 和 γ' 记43的两条支路．于是我们可以分别耦合 β 与 γ，β' 与 γ'，或耦合 β 与 γ'，β' 与 γ．两种耦合都得到图9.11．也可以耦合 β 与 β'，γ 与 γ'．这样得到的是图9.12．于是 $e=2g+h$．图9.11
[253] 与图9.12各只有两个节点．所以按照上述公式，可知 $g=2\cdot3\cdot2=12$，$h=2\cdot2\cdot2=8$．因此 $e=2g+h=32$．其次再拿图9.10来看．它在节点4处有一个自环②．抹掉这个自环，我们得到图9.13，而 $f=2j$．但在图9.13里耦合会于4的两条支路就与图9.11等价．所以，$f=2j=2g=24$．把这些结果代入前段最后的等式中，我们就得到 $a=6e+3f=192+72=264$，所以 $N=15\cdot2^5\cdot a=126720$．这就是一副15张的骨牌按要求排成一行的可能排法的总数．在这个答案里，我们把同一种排列的由左到右和由右到左

① 以下，e，f，g，h，i 分别表示图 9.9～图 9.13 的画法数目．——译者注

② 即，仅有一个节点的闭路．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

看成是两个不同的排列.如果把它们看成是一样的,那么应将上述答数除以2.环形排列的数目是$2^5\cdot a$,即8 448.

我们已经看到一个五边形及其对角线的一笔画法有 264 种.相仿地,对于一个七边形来说,这个数目是 $h = 129\,976\,320$.所以,最大点数达到双六的一副 28 张骨牌按要求排成一行的可能排法的总数是 $28\cdot 3^7\cdot h$,即 7 959 229 931 520.同样,对于一个九边形来说,这个数目是 $n = 2^{17}\cdot 3^{11}\cdot 5^2\cdot 7\cdot 11\cdot 40\,787$.所以,达到双八的一副 45 张骨牌按要求排成一行的可能排法的总数是 $45\cdot 4^9\cdot n$①.

迷　　宫

大家都读到过希腊人米诺斯(Minos)的迷宫和罗莎蒙德(Rosamund)的闺房.各地都有一些现代的迷宫——在汉普顿(Hampton)宫里就有著名的虽然很简陋的一座.很多人都曾摸索到里边过,或者在一座这种建筑里,或者在一张画上.以下我来讲述一种走法.按照这个方式行走,则即使一个人对此种构筑的详图毫无所知,他也能行遍其每个角落.

论述迷宫的理论已包含于上述的欧拉定理里.迷宫里的路
径就是先前所说的支路,两条或几条路径的交会点就是先前所 [254]
说的节点.迷宫的入口,死胡同的终点,以及迷宫的奥室都是悬空端点,因而也都是奇节点.

如果仅有的奇节点是迷宫的入口和奥室,这就要求不存在死胡同,那么这迷宫的路线是可以一笔画成的.这个论断得自欧拉的第三个定理.还有,不论一个迷宫里有多少个奇节点,我们总能够找出一条由入口到奥室而且无重复步子的路线,这种路线一般地只走遍迷宫的一部分.但不论在本段所述的哪种情况

① 这些数字结果也曾经用代数的方法得到过.参看 M. Reiss, Annali di Matematica, Milan, 1871, Vol. Ⅴ, pp.63—120.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

下，都可以把这条路线确定下来而无须知道该迷宫的详图.

无论如何，如果我们采用欧拉的建议并且假定迷宫的每条路径都是双行道，那么，详图是不需要的.在这种情况下，我们能够给出一个确切的法则，按它行事，我们就能走遍任一迷宫的每个角落，即使一点也不知道它的结构.当然，一个迷宫的每条路径都走两遍.这样行事虽然必能到达其奥室，但所走的路线不会是最短的.不过，只要不犯错误，那么一定能走遍迷宫的每个角落，途中必然要经过奥室，而且不会迷路.

我用不着多解释为什么能够走遍一个双行道的迷宫，只要注意这时每个节点都是偶节点，由欧拉的第二定理即知，如果我们从入口开始行进，则必能走遍整个迷宫；中途经过奥室而最后从入口出来.这个走法需要我们把每条路径来回各走一次.

如果迷宫是画在纸上的，那么通向奥室的路线通常是明显的；但是在一个真实的迷宫里，除非知道它的构筑图，要找到正确的路线往往是不大容易的事.为了确保正确地描绘一个不明其构筑的迷宫，需要一些标志我们行走过的路径和所行方向的
[255] 办法.例如，在入口处和每条走过的路径的端点画上一个箭头，或者更好一些是在右边的墙上画一个记号，那样凡是看到两边墙上都有了记号的胡同就不再进去了.

摸索迷宫的各种实际规则中似乎以塔里①发表的最为简单.我要解说的就是它.走过一条路径 PQ 而达到一个节点 Q 之后，再循另一条先前尚未走过的路径 QR 离开 Q 而前进（如果这是可能的）.如果除了 QP 之外，所有其他从 P 出发的路径都已经走过了，或者 Q 是一条死胡同的底，那么就循 QP 折回到 P.

---

① Nouvelles Annales de Mathématiques, 1895, series 3. Vol. XIV, pp. 187—190. 又见 Dénes König, Theorie der endlichen und unendlichen Graphen, New York, 1950, pp. 41—43.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

坚守以上规则,最终你将回到出发点并且把所有的路径都走了一个来回.(注意,迷宫不限于是平面上的.同样的规则能帮助你从地下墓穴里逃出来,只要你有个灯火照亮你自己留在灰尘中的脚印.)

我所说的那种类型的迷宫(例如,一系列交织在一起的路径包含着通向迷宫深处的奥室或隐秘之地的某些路线)在古代或中世纪的建筑中是绝少见的.古人称之为迷宫或迷园的一类东西似乎包括的是那些带有许多地窖和通道的复杂建筑①.那样的建筑也可以叫做迷宫,但不是现代通常所理解的迷宫.上述规则可以帮助任何一个人走遍此类任何建筑.关于罗莎蒙德的闺房,除了德雷顿(Drayton)、布朗姆顿(Bromton)克奈顿(Knyghton)的记载之外,我不知道是否还有其他描述.有些人认 [256]
为,记载中的闺房不过是一所房子,其中的通道错综纷乱.

另一类古代迷宫是局限于一小块地面上的弯弯曲曲的甬道,它通向深处的一棵小树或神龛②.这是一种不会把你引入歧途的迷宫,不过,由于整个面积被仅只一条弯弯曲曲的甬道占满,所以即使迷宫所占的地面不大,从入口到奥室路线的长度是很可观的.

给米诺陶(Minotaur)建造的迷宫的传统形式是此类迷宫的

---

① 例如,希罗多塔斯(Herodotus)卷Ⅱ,148章上关于美利斯湖(Lake Moeris)上迷宫的记述;斯特拉波(Strabo),卷XVII,第1章37节;狄奥多洛斯(Diodorus)卷Ⅰ,第61章、66章;以及普利尼(Pliny)Hist. Nat.,卷XXXVI,第13章,第84—89节.关于这方面以及其他方面的资料见A. Wiedmann, Herodots zweites Buch, Leipzig 1890, p.522以后.又见维吉尔(Virgil)Aeneid,卷V,章5章;奥维德(Ovid) Met. 卷Ⅷ,第5章;斯特拉波卷Ⅷ,第6章.

② 关于古代和中世纪的迷宫,特别是此类迷宫,可参看The Archaeological Journal, 1858, Vol. XV, pp.216—235上特罗洛普(E. Trollope)先生的一篇文章,上边的许多历史资料都是摘自那里的.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

一个典型.它被铸在克诺索斯(Cnossus)钱币的背面上,这种标本并非罕见,其形状如图9.14所示.实质上这个图样和图9.15的性质是相同的,把这个长方形的图绕着一个圆弄弯即可看出.



图 9.14

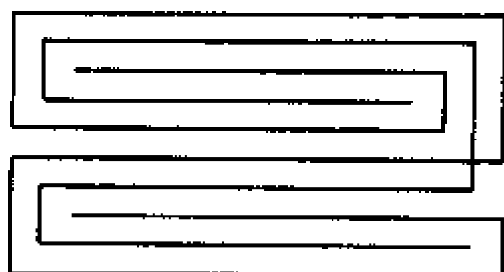


图 9.15

殷沃兹(Inwards)先生曾猜想①克诺索斯钱币上的这个图案可能是祭司们所给表记上的遗迷,它暗示着那里的迷宫的正确路线.取上边的圆形图案,他假定把每个圆弧形隔墙换成夹着一条甬道的等距离的隔墙,从而得到一个迷宫,而原来的图案就是
[257] 这个迷宫的连通图.只要注意当到达一个节点时(即几条甬道的交会点)应进入的甬道是会于节点的诸甬道中与来路隔着一条的甬道,就可以马上明白指示的路线了.这个迷宫也可以按靠右壁走(或靠左壁走)这一简单的规则而出入.这个迷宫也可以用筑起一些增设栅栏的方式予以改进而不影响上述规则的可行性,但不会引起实质的困难.这是个很好的玩具,虽然它所依据的猜想是很自然的,但无史实可查.另一种猜想是:钱币背面的曲线是参加伴乐舞蹈者手中所持飘带的形象.还有人认为这个图案是从流行的卍②字图案逐渐演变来的.

---

① Knowledge, London, October, 1892.

② 图案卍(Swastica)本为佛教表示吉祥之意.女皇武则天定为汉字,读作"万".见《佩文韵府》、《康熙字典》及《辞源》.今有些大字典据一手抄佛经中曾误作卐而将二者并列,混为一谈.后者为近代之纳粹党徽.实大相径庭,以讹传讹.不敢苟同.——译者注

我们必须知道,而且我们必将知道

http://maths352.bokee.com

克诺索斯迷宫图经常被刻在希腊与罗马的珍宝上；类似但更精致的图案则见于罗马的许多镶嵌细工上①.晚代皇帝的朝服上常镶着一个克雷顿(Cretan)迷宫图，显然从那时起又被模仿到许多教堂的墙壁和地板上②.晚些时候，在意大利和法兰西这些壁饰和地饰又被发展为非常复杂的云形涡卷.但就我所知，它们都只是由一条曲线形成的.现在还保存下来的一些最好的

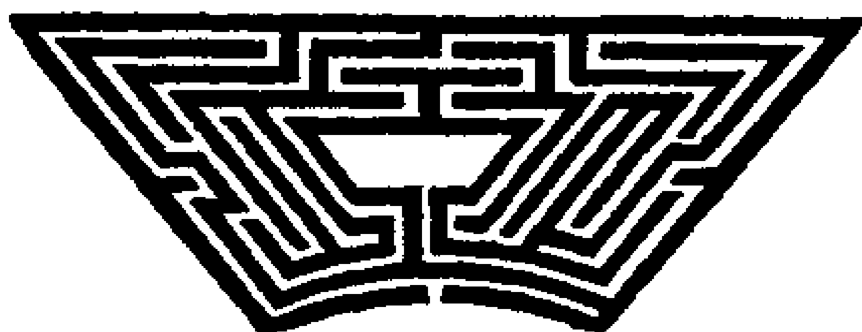


图 9.16 汉普顿宫的迷宫 [258]

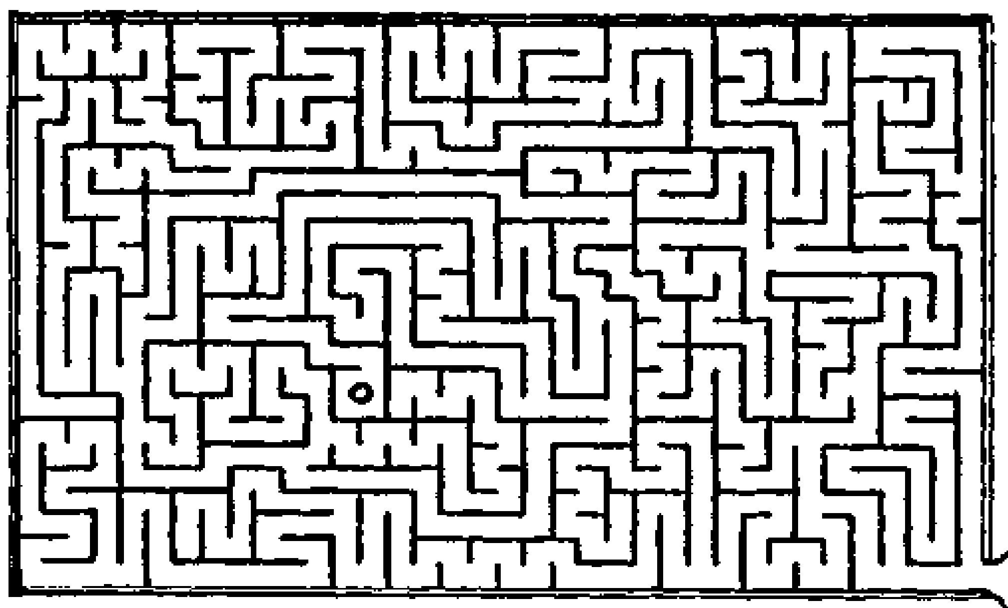


图 9.17

① 参看 Breton 的 Pompeia, p.303.

② Ozanam, Graphia aureae urbis Romae, pp.92,178.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

样品是在卢卡(Lucca),普罗旺斯(Provence)的艾克斯(Aix),以及普瓦捷(Poitiers)的大教堂的墙上;罗马(Rome)的特拉斯梯维尔(Trastevere)的圣玛丽亚(Santa Maria)大教堂、拉韦纳(Ravena)的圣维塔利(San Vitale)大教堂、圣奥默(St.Omer)的圣母院,以及沙特尔(Chartres)大教堂的地板上①.它们可能是用以表示朝山进香似的人生旅程.

在英国,这些迷宫通常甚至可以说总是被凿饰在庙宇或者修道院附近的草皮地上.多少有些理由认为,作为宗教仪式行过它时,在每到一过拐弯的地方都要念一声"圣哉天父"或"万福玛利亚".文艺复兴后,此类迷宫常被称为"特洛伊城(Troy-Towns)"或"朱理安后宫(Julian Bowers)".迄今或不久前尚存的最佳作品所在地可以举出:坎伯兰(Cumberland),罗克利夫马舍斯(Rockliff Marshes);约克郡(Yorkshire),阿森比(Asenby);林肯郡(Lincolnshire),阿尔克波罗(Alkborough);拉特兰郡(Rutlandshire),温(Wing);北安普顿郡(Northamptonshire),布顿-格林(Boughton-Green);剑桥郡(Cambridgeshine),康伯顿(Comberton);埃塞克斯郡(Essex),萨弗伦沃尔登(Saffron Walden);还有温切斯特(Winchester)附近的奇尔科姆(Chilcombe)②.

现代的迷宫似乎起源于文艺复兴时期,可能出自意大利.在英国,图德与斯图亚特王朝所建宫殿的大建筑中都带有迷宫.其中以附属于索思沃克(Southwark)、格林威治与汉普顿宫诸皇宫者因邻近首都而最为著名.最后一个是由伦敦(W.London)与怀斯(Wise)在1690年为威廉三世设计的,他对此种奇物特别爱
[259] 好.在许多导游册子上都给出了它的平面图.它对于大多数观光

① 卢卡、拉韦那皆意大利城市;普罗旺斯为法国一个省;艾克斯、普瓦捷、沙特尔皆法国城市;圣奥默为法国一镇名.——译者注

② 皆英国郡、市名.温切斯特为南安普顿(Southampton)郡之首府.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

者是足够详细的.然而其设计并无奇特之处,因为你只要一直靠一边(左边或右边)走,那是一定可以走遍各处的,并且没有高于三阶的节点.

除非通往奥室的路线在某点处分了叉并且后来这两条叉道又合拢起来而形成围绕奥室的一个圈子,奥室总是可以按上述靠一边走的规则而达到的.能够这样入出的迷宫都够不上一个难字.如果路线分叉如上所述,那么节点愈多、节点的阶数愈高,则迷宫的难度就愈大,特别是如果带有桥梁和涵洞而形成立体的迷宫时.在普通花园里一块不大的地面上要建造这样的迷宫是不容易的.本书 263 页上的图 9.17 是我在自己的花园里建造的迷宫,其路径不超过 36×23 条,注意其中没有高阶节点.

树

欧拉的最早研究限于闭网络.在迷宫问题里假定了有任意多个死胡同,其端底为悬浮节点.现在我们可以更进一步假定图的闭合部分缩退为一个点.得到的结果便是所谓"树".

我们可以用两端带有钩子的细棒来说明树的可能形状.从一根这样的棒开始,我们可以在它的任一端挂上一根或几根类似的棒,挂上的每根棒的另一端又可以挂上一根或几根有钩的棒,等等.每个空钩和每个两根或多根棒相连的点就是至今所说的节点.这些棒就是至今所说的路径或枝. [260]

树的理论创始于凯莱,其文发表于 1856 年[1],当今已成为现代分析的某些分枝中相当重要的部分.理论的阐述已经是解析的而不再是几何的.我想只用给出下列结果就够了.

---

[1] Philosophical Magazine, March 1857, series 4, Vol. XIII, pp. 172—176;或 Collected Works, Cambridge, 1890, Vol. III, no. 203. PP. 242—246;又可参看关于二重分拆的文章,Philosophical Magazine, November, 1860 series 4, Vol. XX, pp.337—341.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

当逐步找出具有 n 个节点的树的个数时($t_1=t_2=t_3=1$, $t_4=2,\cdots$),凯莱观察到具有 n 个"带标号的"节点①的树的个数是 n^{n-2}. 他还研究了具有 n 个节点的"有根的"树,即,特别指定了一个节点为根的树.(这个概念起源于单基取代碳氢化合物的计数.)令

$$t(x)=\sum_{n=0}^{\infty}t_nx^n \quad 与 \quad T(x)=\sum_{n=0}^{\infty}T_nx^n$$

分别表示树与有根树的生成函数(或计数级数),则

$$t(x)=x+x^2+x^3+2x^4+3x^5+6x^6+11x^7+23x^8+\cdots,$$

$$T(x)=x+x^2+2x^3+4x^4+9x^5+20x^6+48x^7+115x^8+\cdots.$$

凯莱与波伊亚②分别得到了函数方程

$$T(x)=x\exp\sum_{r=1}^{\infty}\frac{1}{r}T(x^r)$$

的隐式与显式. 奥特(R.E.Otter)③发现了用有根树数表示树数的最漂亮的公式:

[261] $$t(x)=T(x)-\frac{1}{2}\{T^2(x)-T(x^2)\}.$$

这些结果有其在另一个拓扑问题上的应用:求 n 个圆(或球)相包含或在外的可能方式的数目. 例如两个圆可以相互在外,也可以一个包含在另一个内. n 个圆可以和具有 n 个枝的树的除了根的节点对应起来. 不含于别的圆内的圆对应于直接由一个枝与根相连的节点. 而每个枝表征着一个圆在另一个圆内. 这个对应说明了所求的方式数目正是 T_{n+1}. 图

① J.W.Moon, Counting Labelled Trees (Twelfth Biennial Seminar of Canadian Mathematical Congress), W.Clowes, London, 1970.

② Acta Mathematica, 1937, Vol. LXIII, pp.145—254.

③ Annals of Mathematics, 1948, Vol, XLIX, pp.583—599. 或参看 F.Harary, Graph Theory, Addison-Wesley, Reading, Massachusetts, 1969, pp.187—190, 233—234, 它的附录 3 给出了 n≤10 个节点的一切树图.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

9.18 中(画的是 $n=3$ 的情况)每个树的根都用圆圈与一般节点区别开来.

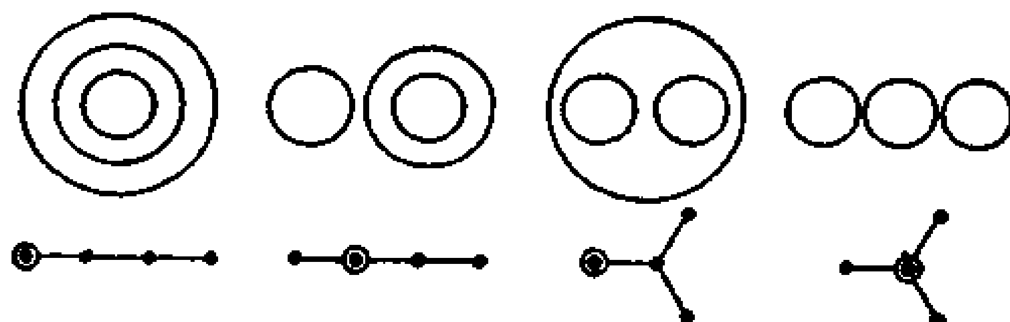


图 9.18

哈密尔顿游戏

以下转到另一类问题:给定一个有节点的几何图形,要求找出一条路线,它通过所有的节点并且每个节点只通过一次.这是本章第一部分所论问题的反问题,并且是一个难得多的问题.

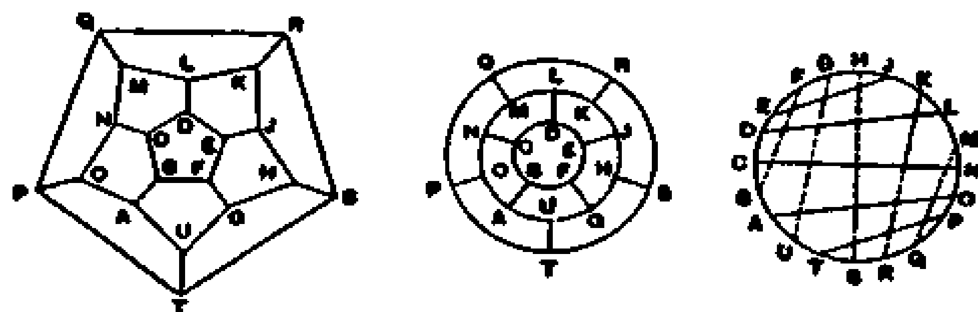


图 9.19

哈密尔顿游戏就是要在一个正十二面体的棱上找出一条路 [262]
线,它通过所有的顶点,并且每个顶点只通过一次.哈密尔顿爵士①发明了这个游戏——如果可以说它是一个游戏的话,他在

① 参看 Quaterly Journal of Mathematics, London, 1862, Vol. V, p.305;或 Philosophical Magazine, January 1884, series 5, Vol. XVII, p.42;或 Lucas, Vol. II. part VII.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

这个多面体的20个顶点旁分别写上一个字母，它们各自代表一个城市的名字．它的30条棱构成唯一可能的路线．用一个立体模型是很不方便的，用这个二十面体在平面上的射影却是很方便的．中间的图和右边的图同样可用以解答我们的问题而画起来要容易得多．

第一个问题是“周游世界”，即，从任一城市出发，要经历每一个城市并且每个城市只去一次而最后要返回到出发地．最先观光的 n 个城市的顺序是指定了的，n 不大于五．

完成这个计划的哈密尔顿规则宣读于1857年在都柏林召开的不列颠联合会上．由上图可看出，解答之一是路线 *ABCDEFGHIJKLMNOPQRSTU*．共有30个解，在十二面体的对称变换下，它们都是等价的．

类似的游戏可以在其他多面体上或平面图上或曲面上的图上进行．哈密尔顿回路与第8章讨论的四色定理的联系是非常有趣的．假定在平面地图上已经画出了一条那样的回路，循着地图上的分界线行走并且每个顶点都只经过一次．回路将平面分成两个区域——内部和外部．跨越内域的任一条分界线把内域分成两个较小的区域，跨越这些小区之一的分界线又把它分成两个更小的区域，如此等等．于是，如果内域里恰有 r 条分界线，那么回路内部的地区就被分成 $r+1$ 个地区．此外，这些地区可以用两种颜色分别涂染使得任两个相邻
[263] 的地区的颜色皆不相同．我们把一个地区染成红色，与它相邻的一个地区就染成绿色，下一个又是红色，等等．因为每一条可能的分界线都把回路内部的区域分成两个地区，所以不会导致矛盾．相仿的道理也适用于回路的外部，它的分区之一的面积是无限大．所以，平面上有哈密尔顿回路的任何地图皆满足四色定理的要求．

泰特曾猜想，在第8章所说意义上的任一标准地图，其中任何两个地区的公共边界不多于一条，必有一条哈密尔顿回路．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

1946 年找到了此一猜想的反例①.格林伯格斯(E.Ya.Grinbergs)最近又找到了此一猜想的更漂亮的反证②.

他的论证如下:考察一个标准地图中一条哈密尔顿回路的内部,假定有 r 条对角线和 $r+1$ 个地区.令具有 j 条边界的地区的数目为 f_j.则组成回路的边界数为

$$N=\sum_{j=2}^{\infty} j f_j-2r=\sum_{j=2}^{\infty}(j-2)f_j+2.$$

再令回路外部的地区中具有 j 条边界者的个数为 f_j'.将上述公式用于回路的外部,则 f_j 换为 f_j' 而 N 的值不变.相减即得

$$\sum_{j=2}^{\infty}(j-2)(f_j-f_j')=0.$$

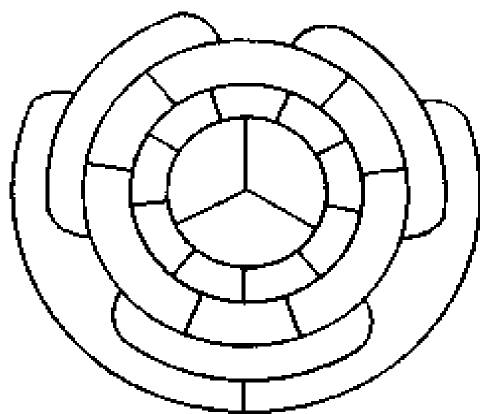


图 9.20

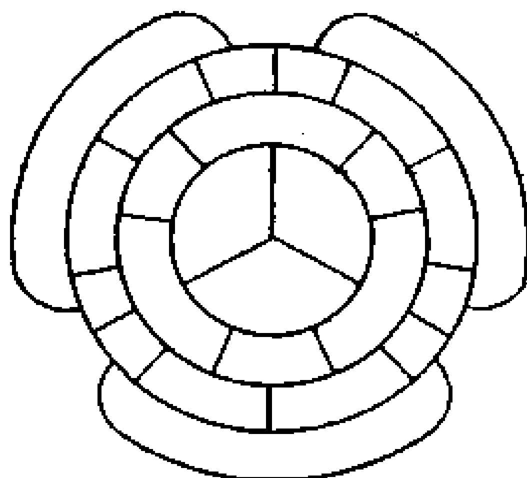


图 9.21

假定我们能够构制一个那样的地图,除了一个地区之外,每个地区的边界数被 3 除时余数为 2.那么上边的等式对于这个地图就不成立,因而此地图不具有哈密尔顿回路.那样的地图事

① W.T.Tutte,"On Hamiltonian Circuits",Journal of the London Mathematical Society,1946,Vol.XXI,pp.98—101.

② Latvian Mathematical Yearbook (Izdat. Zinatne, Riga, 1968),Vol.Ⅳ,pp.51—58.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

实上是可以找到的.图 9.20 就是格林柏格斯绘制的一个例子.这个地图没有少于 5 个地区的环.除了外部的九边形外,它的地区都是五边形或八边形.

[264] 利用同样的方法(并进一步注意当三个六边形共有一个顶点时,任一哈密尔顿回路必把其中之一和其余的两个分开).格林柏格斯曾绘制一个比较简单些的地图,如图 9.21 所示.

C·A·B·史密斯①的一个定理说,在每个顶点皆有三条边相会的网路里,包含一个特定边的哈密尔顿回路的数目必是偶数(可能是零).要证明这个论断,我们先定义:如果通过每个顶点只有一条由地图上的偶数条分界线构成的回路,则这样的一组回路称为一个"泰特链".如果用三种颜色将地图上的分界线进行染色而会于任一顶点的分界线的颜色没有相同的(参看本书第 229 页 ~ 230 页),则称此种染色为"泰特染色".如果两个泰特染色的差异只是三种颜色的一个轮换,那么就认为它们是一样的.容易看出,下列诸命题成立:

(i) 在一个泰特染色里,每两种颜色确定一个泰特链;

(ii) 一个由 m 条回路组成的泰特链可由恰好 2^{m-1} 个不同的泰特染色按此法获得之;

(iii) 由一给定的泰特染色得到的泰特链中包含每条分界线的恰有两个链;

[265] (iv) 一个哈密尔顿回路等价于一个 $m=1$ 的泰特链.

现在来考察包含一条给定的分界线 A 的泰特链的数目,一个由 m 条回路组成的链计算 2^{m-1} 次.据(ii)和(iii),此数为偶数,且是泰特染色数的二倍.但当 $m \neq 1$ 时 2^{m-1} 总是偶数而当 $m=1$ 时它是 1.所以包含 A 的哈密尔顿回路数为偶数.

由史密斯的定理可知,如果所考察的网络有一条哈密尔顿

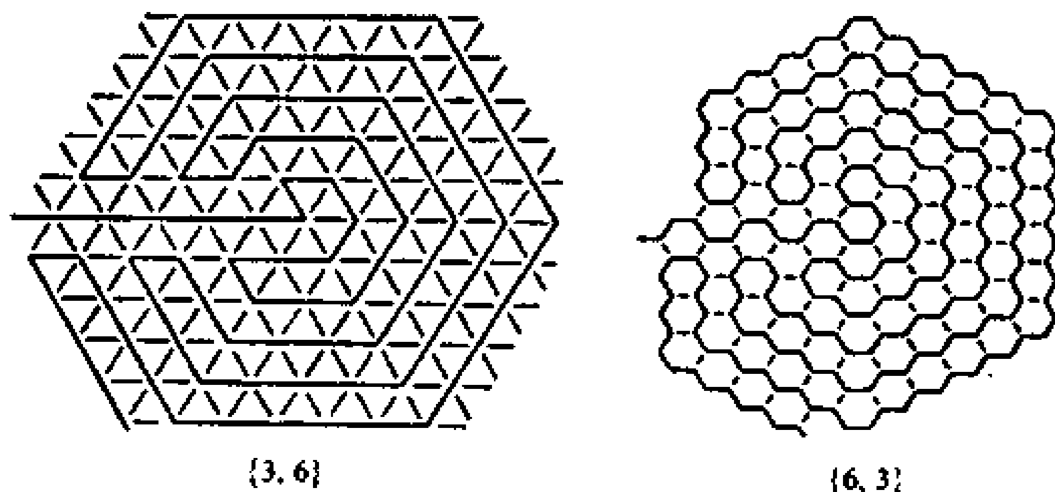
① 史密斯的证明迄未发表.这里的证明取自 W.T.Tutte,"On Hamiltanion Circuits"(见本书第 269 页下的注).

我们必须知道，而且我们必将知道

http://maths352.bokee.com

回路,那么它必至少有三条.

哈密尔顿的问题已被推广到城市数目为无限多的一些情况(所求的路线既无头也无尾).关于沿着正方形铺砌{4,4}的缝线而走的路线,可参看柯尼希(König)的图论的书①.相仿地,它种铺砌({3,6}与{6,3})的处理有如图 9.22 所示.



{3,6}　　{6,3}

图 9.22

棋盘上的马路问题的性质也有些和哈密尔顿游戏相似.关于它,我已在第 6 章中论述过了.

龙　纹　图

平面上另一种无穷多段的路线可以用折叠一个长纸条的方法构成②.从一个平放的长纸条开始,把右边的一半向上折 [266]
起来扣到左边的一半上;然后再把所得的两层纸条照样再折,

① Dénes König, Theorie der endilichen und unendlichen Graphen, Leipzig, 1936, p.32.

② Scientific American, 1967, March, pp.124—125; April, pp.118—120;July, p.115.关于这里引述的许多性质的证明和图形,参看 C.Davis and D.Knuth, Journal of Recreational Mathematics, 1970.Vol.3,pp.66—81, 133—149.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

尽可能地继续折下去.(实际上大约可折七次,但理论上可以永远折下去.)当你把纸条伸开后,它就显出一串有趣的皱折.用 U 记凹下去的折痕,用 D 记凸起来的折痕,就会得到首段如下的序列:

$$UUDUUDDUUUDDUDDUUUDUUDDDUUDDUDDUU$$

其中第一、二、四、八、……个折痕的下边给打上了一个圆点,称为"枢纽".容易看出,第 k 个枢纽的后 k 个折痕与前 k 个折痕正好是相反的,并且,每个枢纽都是一个 U(因为纸条总是往上折的).这两件事实就给我们提供了一个规则,按它写下去,我们愿把序列写多长就可以写多长.还有些别的等效规则,我再说一个.若 $n=2^k m$(m 为奇数),则视 $m\equiv 1$ 或 $m\equiv 3 \pmod 4$ 而知第 n 个折痕是 U 或 D.

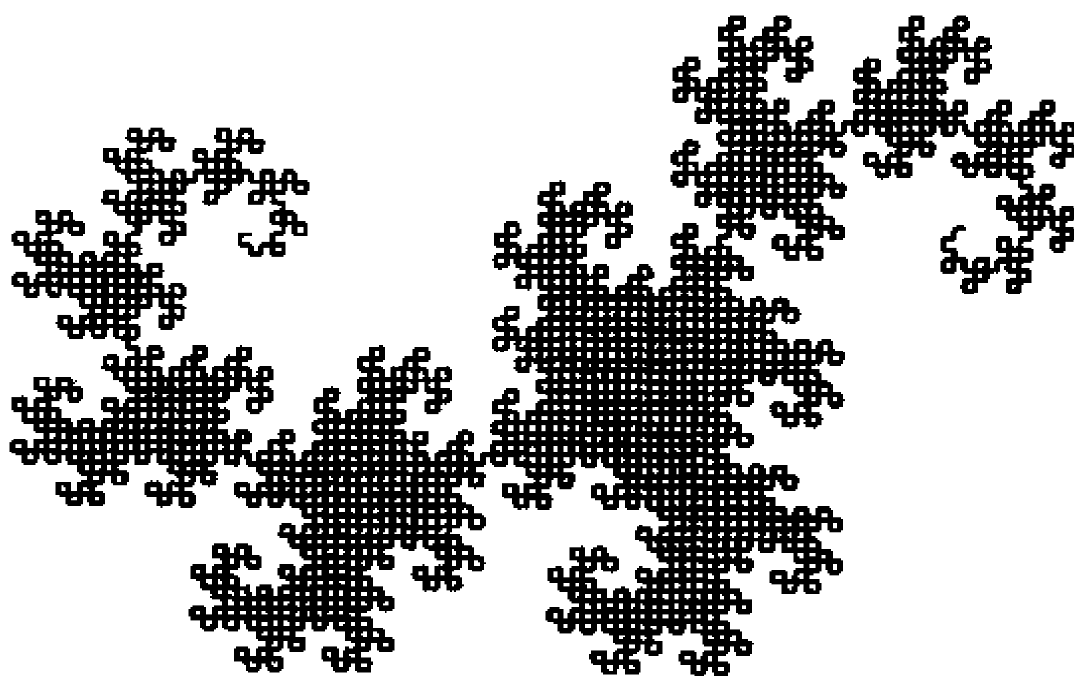


图 9.23

然后将纸在每个折痕处顺着折痕方向折 90°角.所成的形状就是所谓"龙纹",它是一种有趣的爬虫形——沿着铺砌{4,4}的缝的四分之一而走的无穷多段曲折路线(参看图

我们必须知道,而且我们必将知道

http://maths352.bokee.com

9.23).实际上,如果把这个图案绕其起始点转过一个、二个、三个直角而重描在一起,形成从同一点发出的尾接尾的四条龙形,那么这四条龙彼此互不相交.如果在它们之间无止境地重排下去,它们将描出上述铺砌的全部缝线而且恰好描一遍.

如果把龙纹的起始点和第二个角点用直线段连起来,第二个角点和第四个角点用直线段连起来,等等,则这些连线所成的图案和原图案形状相同,只不过放大了$\sqrt{2}$倍并且沿顺时针方向转过45°角. [267]
(这个论断在上述由 U 与 D 构成的无穷序列身上有其相应的事实:如果把序列中所有的第奇数项去掉,剩下的序列和原来的序列是一样的.)由此可见,枢纽都在围绕起始点的等角螺线上.

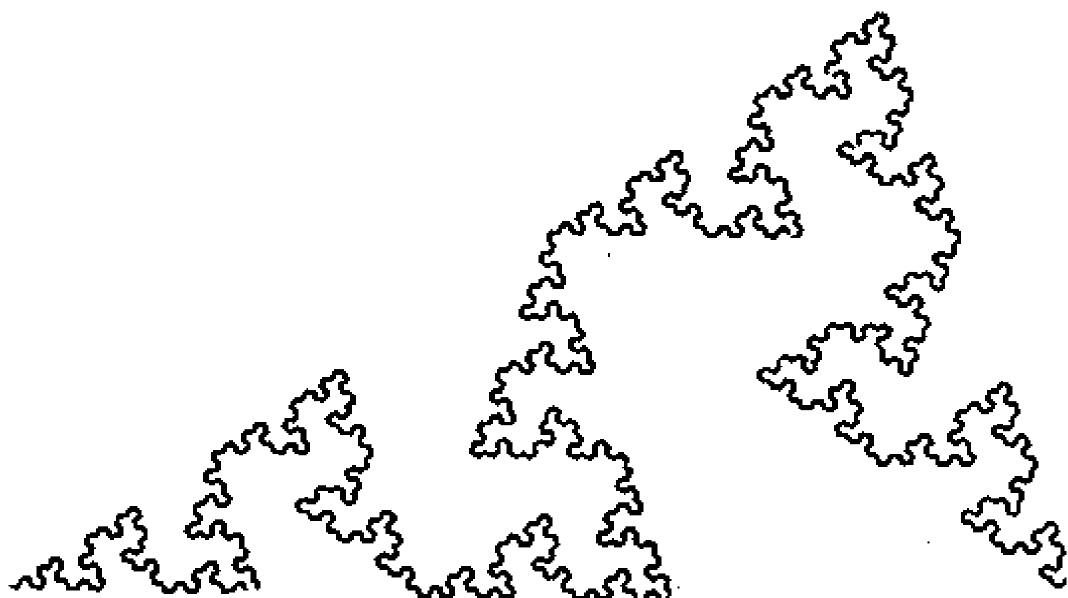


图 9.24

上边的相似性是把龙纹的一些角点去掉而把龙纹"疏松了".反之,我们也可以添进去新的角点把龙纹"致密"而得到一种相似性①.具体地说,将一个已给的龙纹的所有角点都看成边

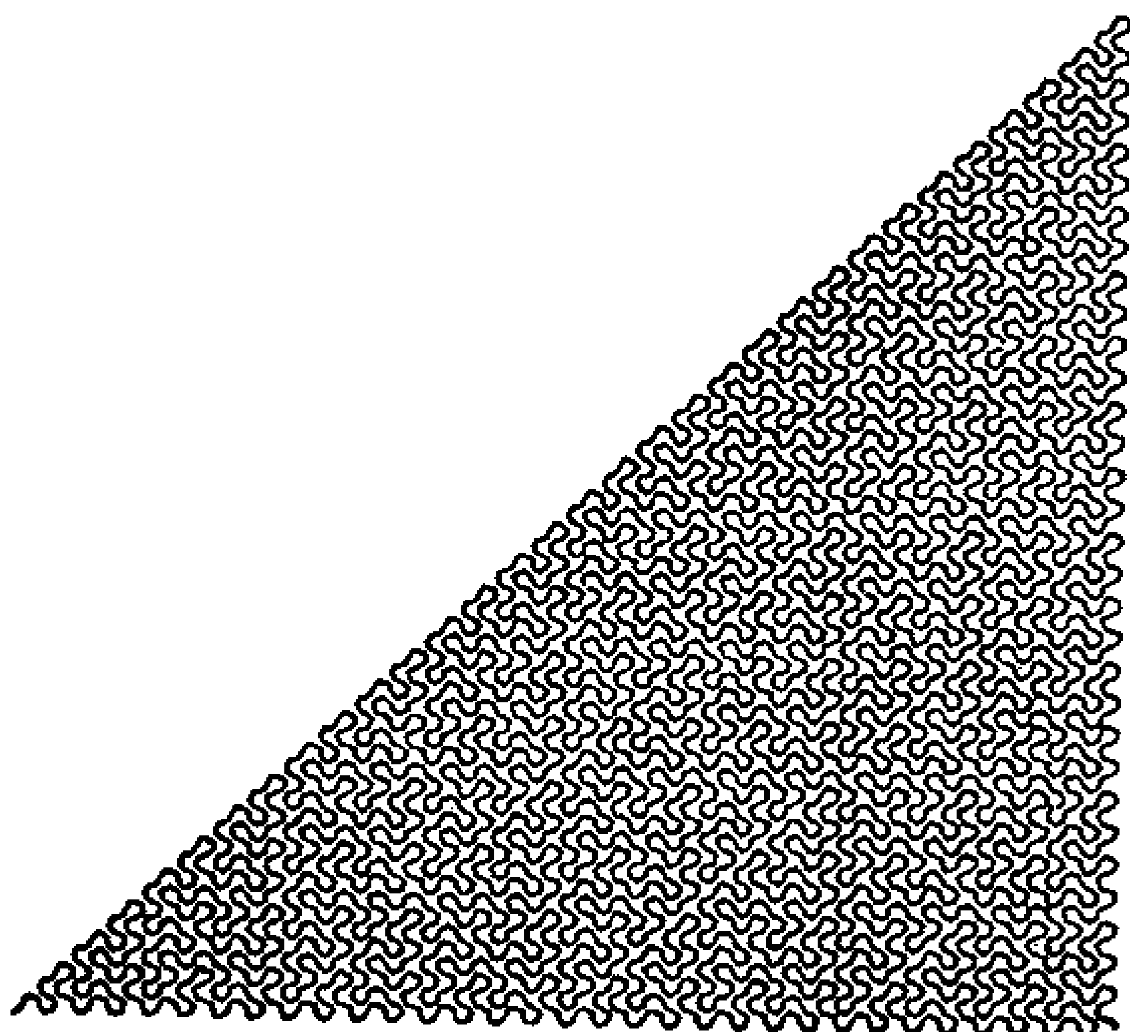
① 由此为契机于近25年来发展出了一个全新的数学分支——分形几何.它包含着不少新的概念、理论、应用和令人赞叹的精美图形.可参看 Benoit B. Mandelbrot, Fractal Geometry of Nature, 1982; Kenneth Falconer, Fractal Geometry, 1990.后者有中译本《分形几何》,1991.——译者注

我们必须知道，而且我们必将知道

[redacted]

长为原龙纹边长的 $1/\sqrt{2}$ 的龙纹的第偶数号角点，就可以画出一个较密的龙纹．不断地进行这一致密过程，就得到一系列愈来愈密的龙纹，它的极限是一条"铺满平面"的曲线①．从同一个点出发的这些极限曲线中的四条曲线把平面上的每个点都通过了．

最初的折纸过程的许多大同小异的折法都被研究过．最简
[268] 单的另一种折法是，不要每一步都向上折而一上一下交替地折．
于是，在折痕的序列中，"枢纽"将交替地居于诸 U 与诸 D 之间；



[269] 图 9.25

① H. Steinhaus, Mathematical Snapshots, New York, 1969, pp. 102—103.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

在枢纽之间，规律仍是枢纽后边的第 k 个折痕与前边的第 k 个折痕的折向相反. 图 9.24 表明纸条的折法是在每个折痕处折一个 108°角的结果. 路线都局限于一个张角为 36°的扇形内，枢纽都交替地位于这个扇形的左、右边界上. 第三个枢纽与起始点之间的距离是第一个枢纽与起始点间距离的 τ^2 倍. 折得再多一些使每个角度都成为 90°，则路线就成为一条一笔画成、永不自交、沿着铺砌{4,4}的一片无限大部分而走的路线. 这个部分恰好是一个张角为 45°的一个扇形，不过沿着右边界的每第偶数段界线都去掉了.（图 9.25 中为了表明路线的走向而把所有的拐角都抹圆了.）①

类似的形象也能够在折三折时得到. 再一次从一个平放的长纸条开始，我们把它在距右端为整个长度的三分之一处向上折，并在距左端为整个长度的三分之一处向下折；然后把折成的结果再这样折下去. 当把纸条打开后，从中心向外读折痕序列的一部分是

$$UDDU\underset{\cdot}{D}DUUDU\underset{\cdot}{D}DU\underset{\cdot}{D}\underset{\cdot}{D} \mid \underset{\cdot}{U}\underset{\cdot}{U}DU\underset{\cdot}{U}DUDDU\underset{\cdot}{U}DUUD$$

枢纽有与前述问题中的枢纽同样的意义，不过它们都出现在每个方向上距中心为 $\frac{1}{2}(3^n+1)$ 的每个折痕处. 当把每个折痕折转 60°时，结果是“三龙纹”，它是一条一笔画成、永不自交并且沿着铺砌{3,6}的界线而走的路线. [270]

① 图 9.23—图 9.25 都是纸条被折好后的侧视图. ——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第10章 组合设计

在本章我们再回到第6章末所提出的一类问题上来.在19世纪,这类问题还只具有娱乐的兴趣,但近来已证实它对统计学家是很有用的.当冯·施陶特(Von.Staudt)发现了仅包含有限多个点的几何的可能性时,一种重要类型的组合设计便在1856年提出了.他的工作虽被遗忘了四十年之久,但其思想今已硕果累累.

一个射影平面 一位女士想邀请她的七位朋友参加一系列的宴会.她的餐桌除了她本人外只有三个空位.另外,这位女士想让她的每两个朋友只在餐桌上相见一次.因此就提出这样的问题:在以后的几天里应该如何安排她的邀请?现在让我们用a,b,c,d,e,f,g表示她的朋友的名字,而用1,2,3,…表示宴会在哪天举行.

不失一般性,我们假定她第一天邀请的是a,b,c;否
[271] 则,我们可把她的朋友重新命名.然而,在安排第二天的邀请时,这位女士遇到了困难.她是应该邀请集合$\{a,b,c\}$中的一位加上两位新朋友,还是全邀请新的一组朋友,如$\{d,e,f\}$?下面要说明,如果第二天她采用了邀请$\{d,e,f\}$的方案,那么她就会陷入困境.事实上,在以后的几天里,她就得让g与$\{a,b,c\}$中的一位和$\{d,e,f\}$中的一位同桌,而这只能安排在第3,第4或第5天.此后她所有可能的组合方案就都用完了(否则,就不满足两位朋友只相见一次的要

我们必须知道,而且我们必将知道

http://maths352.bokee.com

求).这可以从图 10.1 中看出,在第 6 天就找不到一个人不曾和譬如说 a 或 e 同过桌.因此,用这种安排方法是不可能达到目的的.

因而结论是:第二天应选择其他可能的邀请方案.事实上,我们已经证明,在任何不同的两天中,应有一个相同的客人.一旦知道了这一点,给出正确的邀请方案就不难了,而且可以看到共需七天.作为例子,我们给出一种方案:

第几天:	1	2	3	4	5	6	7
邀请的客人:	a	a	a	b	b	c	c
	b	d	f	d	e	d	e
	c	e	g	f	g	g	f

这张表也可以用几何方法来表示,如图 10.2.其中朋友用点代表,第几天用线代表.图形中的七个点和七条线是这样联结的:任何一条线连接着三个点;任何一个点都在三条线上;任何两个点都在一条线上;任何两条线都有一个公共点.这些点和线便构成了一个二阶的射影平面,记之为 PG(2,2),其精确的定义在第 289 页给出.

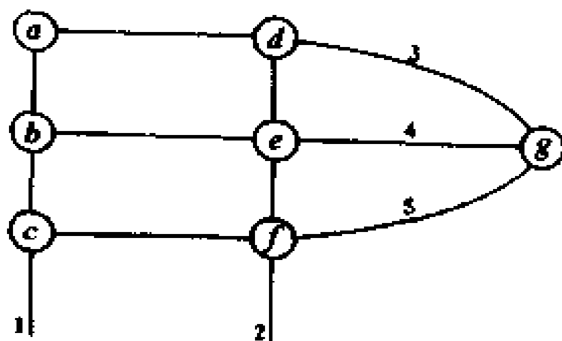


图 10.1

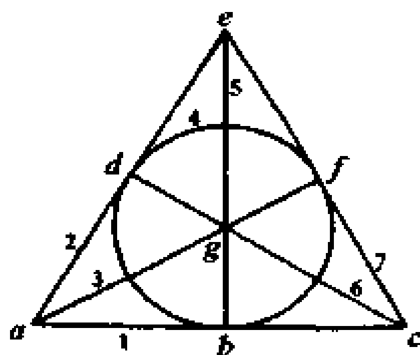


图 10.2

关联矩阵 有一个代数方法能表示上述点与线之间的关系(就是朋友和第几天的关系).这种点-线关系的关联矩阵 N 是由 7×7 个元素组成的,这些元素根据相应的点是否落在相应的线上,分别取值 1 或 0: [272]

我们必须知道，而且我们必将知道



$$\begin{array}{c}\begin{matrix}1&2&3&4&5&6&7\end{matrix}\\ N=\begin{pmatrix}1&1&1&0&0&0&0\\1&0&0&1&1&0&0\\1&0&0&0&0&1&1\\0&1&0&1&0&1&0\\0&1&0&0&1&0&1\\0&0&1&1&0&0&1\\0&0&1&0&1&1&0\end{pmatrix}\begin{matrix}a\\b\\c\\d\\e\\f\\g\end{matrix}.\end{array}$$

矩阵 N 也能反映出射影平面的性质:每列都包括三个 1,每行也都包含三个 1;每两行都有一个共同的 1,每两列也都有一个共同的 1. 如果把点和线相互置换,这种性质仍将保留.例如,把 N 变换成:

$$\begin{array}{c}\begin{matrix}7&2&3&5&1&6&4\end{matrix}\\ N'=\begin{pmatrix}0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\\1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\1&0&1&0&0&0&1\\1&1&0&1&0&0&0\end{pmatrix}\begin{matrix}a\\g\\b\\c\\d\\f\\e\end{matrix}.\end{array}$$

要注意,矩阵 N 是对称的,而置换阵 N' 却是非对称的.但矩阵 N' 是一个循环阵,这不难从相邻的两行之间的关系看出.因此,N' 又可以定义为:

$$N'=\mathrm{circ}(0\ 1\ 1\ 0\ 1\ 0\ 0).$$

一个阿达玛矩阵 这位女士七次宴会都参加了.假如第 8 天举行一次 8 个人都参加的告别宴会,这相当于给关联矩阵 N
[273] 增加一行一列而构造成一个 8×8 的矩阵 F:

$$F=\begin{pmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&0&0&0&0\\1&1&0&0&1&1&0&0\\1&1&0&0&0&0&1&1\\1&0&1&0&1&0&1&0\\1&0&1&0&0&1&0&1\\1&0&0&1&1&0&0&1\\1&0&0&1&0&1&1&0\end{pmatrix},\quad H=\begin{pmatrix}-&-&-&-&-&-&-&-\\-&-&-&-&+&+&+&+\\-&-&+&+&-&-&+&+\\-&-&+&+&+&+&-&-\\-&+&-&+&-&+&-&+\\-&+&-&+&+&-&+&-\\-&+&+&-&-&+&+&-\\-&+&+&-&+&-&-&+\end{pmatrix}.$$

我们必须知道，而且我们必将知道

现令 J 代表一个 8×8 矩阵，其元素均为 1，而令 I 为一个 8×8的单位阵，其主对角元均为 1，其余元素取零．则 $H=J-2F$，且有如下的性质①：

$$HH^T=8I$$

这表明 H 的任何两个不同的行向量的内积为零(所谓两个行向量的内积是指对应分量的乘积之和)，而任何一行自身的内积等于矩阵 H 的阶数．具有这种性质且元素取值 $+1$ 和 -1 的矩阵，用雅克斯·阿达玛(Jacques Hadamard)的名字命名，叫做阿达玛矩阵，在 110 页曾把它们叫做半条反拼砌(anallagmatic pavements)，并且就它们的简单结构加以描述．

一例纠错码　把上面的 8×8 矩阵 F 和其补 $J-F$ 合在一起，便得到一个 8×16 的矩阵：

$$\begin{matrix} & \begin{matrix}1&2&3&4&5&6&7&8&9&10&11&12&13&14&15&16\end{matrix} \\ G^T= & \begin{pmatrix}1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1\\1&1&0&0&1&1&0&0&0&0&1&1&0&0&1&1\\1&1&0&0&0&0&1&1&0&0&1&1&1&1&0&0\\1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1\\1&0&1&0&0&1&0&1&0&1&0&1&1&0&1&0\\1&0&0&1&1&0&0&1&0&1&1&0&0&1&1&0\\1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1\end{pmatrix}.\end{matrix}$$

[274]

考虑这 16 列，每列都有 8 个坐标分量，我们把每两列的对应坐标分量取值不同的个数，定义成这两列之间的“距离”．可以看出：任两列之间的距离不为 4 便为 8．矩阵 G 的 16 个列所构成的集合，由于它的两列间的距离不小于 4，使得它成为一种十分有用的编码．

令 G 的每列作为信息通讯中的一个二进制码的字．由于传

① 方阵 A 的转置 A^T，关于 A 的主对角线折转便可得到．若 H 是对称的，则显然有 $H^T=H$．

输通道的不够完善或许会出现这种情况:发出的正确信息,接收时却会产生一个或多个错误.例如,接收到一个列码(1 1 0 1 1 0 0 1),并假定发生的错误不多于一个,则从码字间的距离考虑,接收者可推断出发射的应是第七列.从而就能纠正任何只含一个错误的码字,并且能检测(而不是纠正)两个错误的出现.因此,这种编码制叫做纠 1 检 2 码.

上面所说的这种码制为一种线性的(8,4).意思是说:如果像第 36 页那样,对 G^T 的列作模 2 的加法运算,即

$$0+0=0, \quad 0+1=1+0=1, \quad 1+1=0$$

则不难证明,G^T 的各列都可表为第 2,第 3,第 4,第 5 列的线性组合.事实上,若用 col 代表列,则有:

$$\text{col } 1=\text{col } 2+\text{col } 3+\text{col } 4, \quad \text{col } 6=\text{col } 3+\text{col } 4+\text{col } 5,$$
$$\text{col } 16=\text{col } 4+\text{col } 5, \quad \text{col } 9=\text{col } 4+\text{col } 4, \text{等等}.$$

所以,我们这种编码有如下特征:G^T 的 16 个列是由其中 4 个独立的列线性张成的,每列有 8 个坐标分量.换言之,我们的编码是八维向量空间中的一个四维子空间,其坐标是二进制数.

我们还可以从上面的编码得到一种(7,4)线性码,为此只要从矩阵 G^T 中删去任一行,譬如第一行.因为余下的字长为 7 的 16 个列仍然是由 4 个独立的列线性张成.由于任何两列至少有 3 个不同的坐标,故(7,4)码是一种纠 1 码.除此之外,这种码还
[275] 有一个显著的特点:到任何一个给定码字的距离为 1 且不属于该码集的(坐标取值为 0 或 1 的)七维向量的数目是 7.而由于该码集共 16 个码字,因而到任何一个码字距离至多是 1 且字长是 7 的向量共有 $16\times(1+7)=128$ 个,这正好是字长为 7 的全部二进制码的个数.用几何上的语言来讲就是:以我们的四维子空间中的码字为球心,以 1 为半径所作的单位球族,在七维的矢量空间中是既没重叠又没漏洞的把整个空间填满.所以把这种码叫做完备码

一例区组设计 让我们再次考察上面的矩阵 G^T.我们删去

我们必须知道，而且我们必将知道

它的第 1 列和第 9 列，便得到一个 8×14 的矩阵 M. 该矩阵有如下性质：每列都有 4 个零和 4 个 1，即

$$M=\begin{pmatrix}1&1&1&1&1&1&1&0&0&0&0&0&0&0\\1&1&1&0&0&0&0&0&0&0&1&1&1&1\\1&0&0&1&1&0&0&0&1&1&0&0&1&1\\1&0&0&0&0&1&1&0&1&1&1&1&0&0\\0&1&0&1&0&1&0&1&0&1&0&1&0&1\\0&1&0&0&1&0&1&1&0&1&1&0&1&0\\0&0&1&1&0&0&1&1&1&0&0&1&1&0\\0&0&1&0&1&1&0&1&1&0&1&0&0&1\end{pmatrix}.$$

而且还可以看到：每行恰有 7 个零和 7 个 1，并且每两行都有 3 个相同的 1 和零. 矩阵 M 正是“区组设计”中的点块关联矩阵，其中

$$v=8,\quad b=14,\quad k=4,\quad r=7,\quad \lambda=3;$$
$$JM=4J,\quad MJ=7J,\quad MM^T=4I+3J.$$

其意义是：我们有一个包含 8 个点的集合，从这 8 个点中取出某 4 个点构成一个区组，要求每个点都落在 $r=7$ 个区组中，任一对点都落在 $\lambda=3$ 个区组中，任三个点都落在一个区组之中，这样的区组共有 $b=14$ 个.

下面我们举例说明这个区组设计. 用正立方体的 8 个顶点表示已知的 8 个点，让 4 个点所构成的 14 个区组为：正立方体的 6 个面，6 个对角面和由其顶点确定的两个正四面体. 若用模 2 加法也许会得到一个更好的表达（这里的所谓模 2 加法就是二进制加法），于是四面体也变成平面. 从图 10.3 可以看出这种 [276]
做法. 14 个区组能用 14 个平面来表示，其方程为：

$$x=0,\quad y=0,\quad z=0,\quad x+y=0,\quad x+z=0,$$
$$y+z=0,\quad x+y+z=0,\quad x=1,\quad y=1,\quad z=1,$$
$$x+y=1,\quad x+z=1,\quad y+z=1,\quad x+y+z=1.$$

它们可用模 2 同余的概念来解释.

这里所讨论的区组设计也可以看成是前面射影平面的一个推广.事实上,当用模2同余表示正方体时,任一点,譬如(0,0,0),都有7条线和7个面通过.它们的关联矩阵与2阶的有7个点和7条线的射影平面相同,这也说明了图10.2与图10.3的相似性.

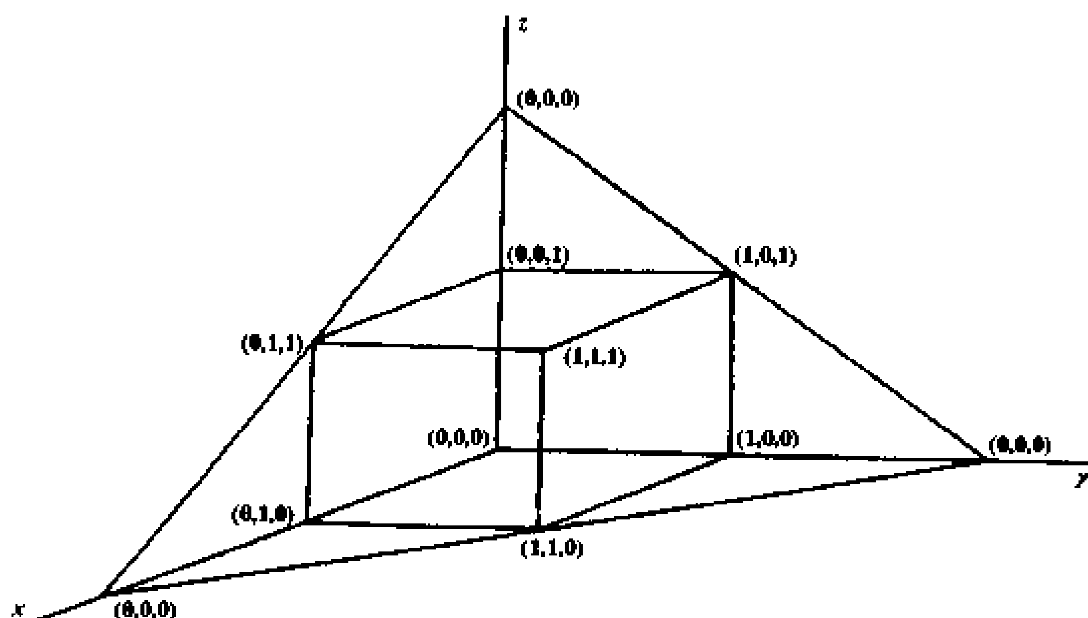


图 10.3

我们已经看到在 8×14 矩阵 M 中,任两行都有三个同列的1.现在让我们看看列之间有什么关系.很显然,对于任一列都有一列和它没有共同的坐标,而其余12列中的任一列都有两个和它同行的1①.我们用一个图中的14个顶点来表示14个列,并把没有同行的1的列所对应的点叫做相邻的点.则便得到所谓
[277] 的梯状图(ladder graph),见图10.4.反之,若把有同行的两个1②的列所对应的点叫做相邻的点,则可得到上面梯状图的补,有时又把它叫做鸡尾酒会图(cocktail-party graph),因为在鸡尾酒会上,假定每个人都要与除了他的同伴之外的每个人交谈.

---

① 此时也必有两个相同的零.——校者注

② 此时也必有两个相同的1.——校者注

我们必须知道,而且我们必将知道

http://maths352.bokee.com

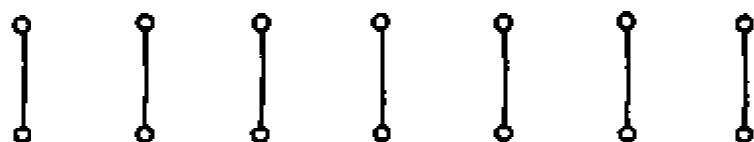


图 10.4

施泰纳三元组 回到我们最初所提出的问题.还记得那位女士的餐桌能提供 $k(=3)$ 个座位(她本人除外),并且她的每两位朋友在 $\lambda(=1)$ 次宴会上相遇.那么,如果她的朋友多于七个,她又该怎么安排呢?

二阶的射影平面是这样的一个区组设计:有 $v(=7)$ 个点,$b(=7)$ 个区组(或线),任何一点都落在 $r(=3)$ 个区组之中,任何区组都有 $k(=3)$ 个点,每一对点都在 $\lambda(=1)$ 个区组中.试问还存在其他的 $k=3,\lambda=1$ 的区组设计吗?也就是对包含有 v 个点的集合,这些点的每三个作为一组,使任何两个点恰好在一个区组之中.假如这些三点一组的集合存在,便称之为 v 阶施泰纳三元组,简记为 $S(v)$,它是以雅各·施泰纳(Jacob Steiner, 1796—1863)①的名字命名的.然而,正如我们将要看到的,他并不是第一个提出这类问题的人.

假若存在一个 v 阶施泰纳三元组.则任一给定的点与其他 $v-1$ 个点中的每一个只在一个三元组中共处一次,因此该点将出现在 $\frac{1}{2}(v-1)$ 个三元组中,而所有三元组的数目是该数的 $\frac{1}{3}v$ 倍,即 $\frac{1}{6}v(v-1)$.由于这两个数都是整数,因此我们便可得到 $S(v)$ 存在的必要条件是:v 被 6 除时余数为 1 或 3.所以 $v=7$, 9,13,15,…而穆尔②在 1893 年证明了这个条件也是充分的.因 [278]

① J.Steiner, Journal für die reine und angewandte Mathematik, 1853, Vol. XLV, pp.181—182.

② Marshall Hall, Jr., Combinatorial Theory, Waltham, Mass., 1967, p.239.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

此施泰纳三元组的存在性问题已被解决(我们曾考虑了 $v=7$ 的情况).

这儿有一个唯一的 9 阶施泰纳三元组①. 它的 9 个点记为 a,b,c,d,e,f,g,h,i，它有 12 个三元组，如图 10.5 所示. 这 12 个三元组是：三行为 abc，def，ghi；三列为 adg，beh，cfi；三条正向对角联线为 aei，bfg，cdh；三条反向对角联线为 afh，bdi，ceg(就像计算三阶行列式那样).

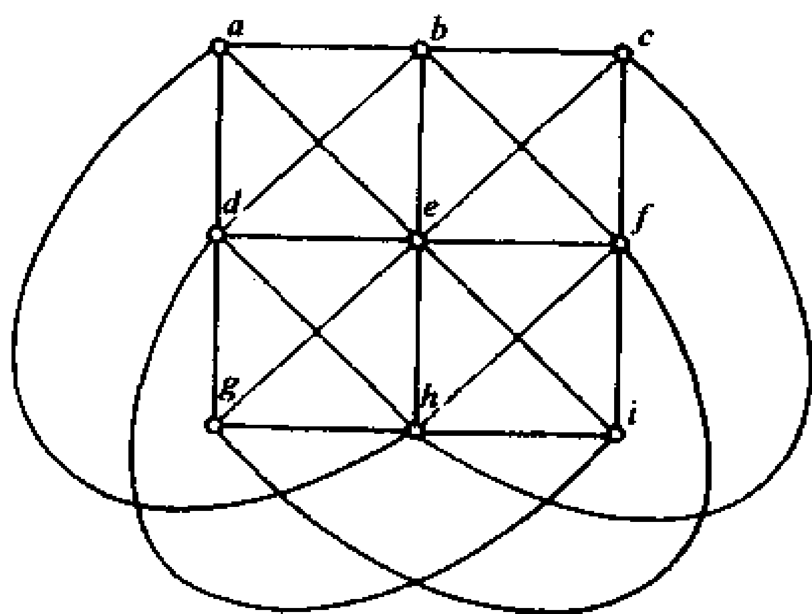


图 10.5

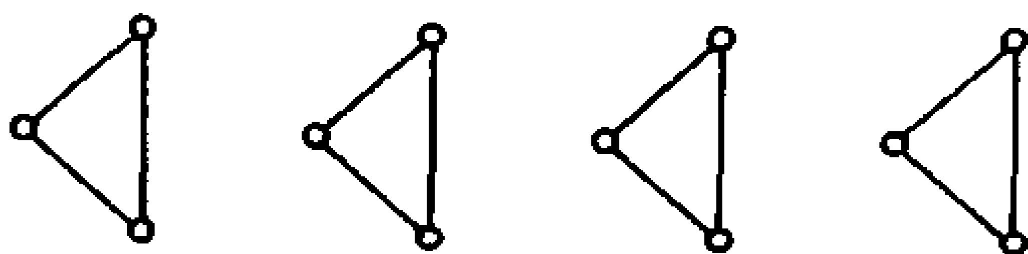


图 10.6

① Cf. G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, Theory and Applications of Finite Groups, Dever, New York, 1961, p. 335.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

任何一点在四个三元组中，任何两点在一个三元组中。共有四簇，每簇包含三个由“平行线”(即无公共点)组成的三元组。这十二个三元组的相互关系由图 10.6 所表示的 12 个点的图形给出。相邻被定义为没有公共部分。 [279]

另一种施泰纳三元组其相应的参数为：

$$v = 13,\quad b = 26,\quad r = 6,\quad k = 3,\quad \lambda = 1.$$

这时存在两个施泰纳三元组，其中的一个是由 13×26 的点块关联矩阵 N 来决定，N 的形式为：

$$N = [N_1 \quad N_2]$$

其中 N_1 和 N_2 皆为 13 ×13 的循环矩阵，分别为：

$$N_1 = \mathrm{circ}(1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0),$$

$$N_2 = \mathrm{circ}(0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0).$$

从 $S(13)$的参数可以看出：给定的任一点 P 和一个与它不关联的三元组 l，则过 P 与 l 相交的恰有 3 个三元组，而过 P 与 l 不相交的也恰有 3 个。在 9 阶和 7 阶的施泰纳三元组中，相应的数目分别为 3，1 和 3，0(见图 10.7)。

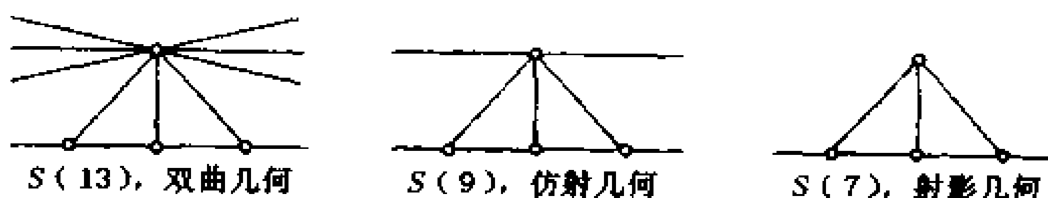


图 10.7

$S(13)$，$S(9)$，$S(7)$中的这种点和块的性质，正好分别与双曲的(或非欧几里得的)①，仿射的(或欧几里得的)，和射影的(或椭圆的)平面几何学中的点和线之间的基本公理一致。其中双曲的非欧几何学是由高斯(1777—1855)、罗巴契夫斯

① 参见 Coxeter，Introduction to Geometry，2nd ed.，New York，1969，chapters 15，16.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



基(Lobachevsky,1793—1856)和波尔约(1802—1860)各自独立发现的.因此,我们把 $S(13)$,$S(9)$,$S(7)$分别叫做有限的双曲平面,有限的仿射平面(见后面的定义),有限的射影平面.

让我们对这些有限平面中的点和线(=块)的进一步的性
[280] 质作一番研究.由于它们是施泰纳三元组,故任何两个不同的点决定了唯一的一条线.而且,这些有限平面关于点是可递的,也就是:任给定两点 P 和 Q,存在点集的一个置换,它映点 P 到 Q,线到线,并且保持点线之间的关联关系不变.对于 $S(7)$和$S(9)$,从图 10.2 和图 10.5 是容易看出这一性质的.而对于$S(13)$,当然对于 $S(7)$也一样,从它的点块关联矩阵 N 的循环性也可推出这种可递性.(值得注意的是,对任意给定的两条线 l 和 m,并不总是存在一个保持关联性不变的置换,它映 l 到 m.)前面我们已经指出,$S(13)$是两个 13 阶的施泰纳三元组中的一个;而另一个由于它对点没有可递性,故无多大意义.

下面的情况是对应于参数

$$v=15,\quad b=35,\quad r=7,\quad k=3,\quad \lambda=1$$

的施泰纳三元组.这些三元组由科尔、怀特(A.S.White)和卡明斯(L.D.Cummings)①彻底解决.结果是:共有 80 个非同构的三元组 $S(15)$,其中有很多关于点是不可递的.然而,在可递的那些三元组中,有 7 个具有另外的显著特点,即它们是柯克曼(T.P.Kirkman)系统,这个概念将在后面讨论.

对于更高价的施泰纳三元组 $S(v)$来说,它们的数目增长很快.例如当 $v=31$ 时,有比 2×10^{15}还要多的非同构的 $S(31)$.

有限几何学 在前面(第 276 页)所介绍的有限射影平面满

---

① F.N.Cole, A.S.White, and L.D.Cummings, Memoirs of the National Academy of Sciences (U.S.A.),1925,Vol. XIV,第二篇报告,p.89.

我们必须知道，而且我们必将知道



足下述的公理：

（1）任何两个不同的点有唯一的直线连接；

（2）任何两条不同的直线有唯一的交点；

（3）存在这样的四点，其中没有任何三点共线；

（4）点的数目是有限的. [281]

更为一般地说，有限射影平面就是一组满足上述公理的点、线以及它们之间的关联关系. 让我们考虑四个点 P,Q,R,S，其中任何三点都不共线，公理(3)保证这样的点存在. 直线 RS 上包含有限多个点，譬如 $q+1$ 个点. 则根据公理(1)，和 RS 不关联的任何点至少落在 $q+1$ 条直线上，而根据公理(2)，最多也只能落在 $q+1$ 条直线上，因此只能在 $q+1$ 条直线上. 特别是对 P,Q 也是如此. 这意味着由 P,Q,R,S 决定的每条直线包含 $q+1$ 个点. 因此，射影平面上的每个点都落在 $q+1$ 条直线上. 射影平面上的每条直线都包含 $q+1$ 个点. 射影平面上点的总数为 $1+q(q+1)=q^2+q+1$，而整个射影平面上的直线总数也为 q^2+q+1.

以上的观察结果和 q 阶有限射影平面的定义，可以追溯到冯·施陶特①. 实际上，有限射影平面是由法诺(Gino Fano)②构造的(对素数 q)，而维布伦(O. Veblen)和伯西(W. Bussey)③对 q 的素数幂构造了有限射影平面. 人们只对 q 的素数幂构造出射影平面，并且也知道(与以前比较而言)不存在 6 阶的射影平面，而下一个非素数幂的合数为 10，而 10 阶的射影平面是否存

---

① K. G. C. von Staudt, Beiträge zur Geometrie der Lage, Vol. I, Nüronberg, 1856.

② G. Fano, Giornale di Matimatiche, 1892, Vol. XXX, pp. 114—124.

③ O. Veblen and W. Bussey, Transactions of the American Mathematical Society, 1906, Vol. Ⅶ, pp. 241—259.

http://maths352.bokee.com



在，尚且不知.

现在我们就阶数为 $q=p^n$（p 是素数）的射影平面，给出一种构造方法. 我们从有 p^n 个元素的伽罗瓦域 $GF(p^n)$ 出发，这个概念曾在前面（第 76 页）讨论过. 现考虑①伽罗瓦域中的两种类型的有序三元组，分别记为

$$(x_1, x_2, x_3) \text{和} [X_1, X_2, X_3],$$

其中 $x_1, x_2, x_3, X_1, X_2, X_3$ 都是 $GF(p^n)$ 中的元素. 我们去掉点
[282] $(0,0,0)$ 和 $[0,0,0]$，并把两个同类型成比例的三元组视为相同，即在几何上视为一点. 所有三元组

$$(\lambda x_1, \lambda x_2, \lambda x_3), \quad \lambda \neq 0, \quad \lambda \in GF(p^n)$$

表示一个点，当然，它与给定的三元组 (x_1, x_2, x_3) 等同. 而令所有三元组

$$[\Lambda X_1, \Lambda X_2, \Lambda X_3], \quad \Lambda \neq 0, \quad \Lambda \in GF(p^n)$$

表示一条线，它与 $[X_1, X_2, X_3]$ 等同. 点线之间的关联定义为：

$$x_1X_1 + x_2X_2 + x_3X_3 = 0.$$

不难看出，由这组点、线和它们之间的关联关系构成的系统，满足我们提出的几条公理. 事实上，两条直线 $[A_1, A_2, A_3]$ 和 $[B_1, B_2, B_3]$ 有一个公共的交点 (x_1, x_2, x_3)，它由方程组

$$x_1A_1 + x_2A_2 + x_3A_3 = 0,$$
$$x_1B_1 + x_2B_2 + x_3B_3 = 0$$

所决定. 两个点 (a_1, a_2, a_3) 和 (b_1, b_2, b_3) 有唯一的一条直线 $[X_1, X_2, X_3]$ 连接，该直线由方程组

$$a_1X_1 + a_2X_2 + a_3X_3 = 0,$$
$$b_1X_1 + b_2X_2 + b_3X_3 = 0$$

所决定. 点的数目是有限的；而且有点 $(1,0,0)$，$(0,1,0)$，$(0,0,$

① H.S.M. Coxeter, Projective Geometry, University of Toronto Press, 1974, p.112.

我们必须知道，而且我们必将知道

http://maths352.bokee.com



1)和(1,1,1)满足公理(3).从而便得到一个 p^n 阶的有限射影平面①,记之为:PG(2,p^n). $p^n=2$ 的情形便是我们讨论过的 2 阶射影平面,已在前面的图 10.2 中作了解释.在 $p^n=3$ 时,伽罗瓦域 GF(3) = {0,1,-1},其上的运算是通常的乘法和下述加法:$1+1=-1$,$-1-1=1$,$1-1=0$.如果用 + 代表 1,- 代表 -1,便得到图 10.8 中所表示的 13 个点和线.

至于域 GF(p^n)上的有限仿射平面,我们把它记为 AG(2,p^n),它是从 PG(2,p^n)的点和线中删掉任意一条直线和其上的点得到的.例如AG(2,3)(图10.5),是从PG(2,3)中删去直线

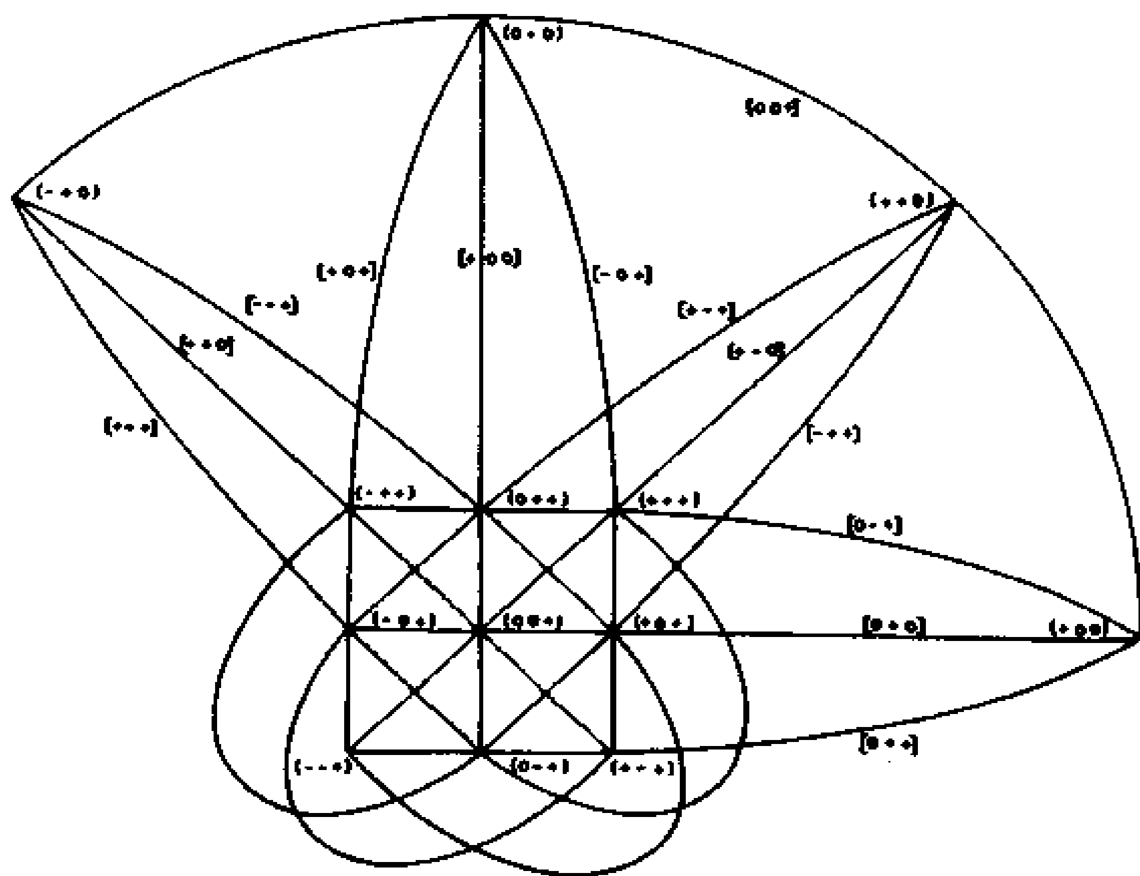


图 10.8

① 采用更复杂的代数系统,可构造出其他射影平面.参看 M.Hall, Theory of Groups, New York, 1959, p.346.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[0,0,1]和其上的点所得到的. 因而所得到的 AG(2,3)的九个点可以只用其前两个坐标表示,因为第三个坐标可规范化为 1.
[283] 对任意的 $p^n = q$, AG(2, p^n)的 q^2 个点和 q^2+q 条线可分别用序偶(ξ,η)和方程

$$\alpha\xi+\beta\eta+\gamma=0$$

表示,其中 $\xi,\eta,\alpha,\beta,\gamma$ 遍历 GF(p^n)的元素.

利用伽罗瓦域也可以构造出高维的几何学. 对于三维空间,我们考虑由 GF(p^n)的元素构成的四元序组(x_1, x_2, x_3, x_4)和[X_1, X_2, X_3, X_4],这两类成比例的四元序组分别给出三维空间中有限射影空间 PG (3, p^n) 的点和面. 点、面之间的关联由式

$$x_1X_1+x_2X_2+x_3X_3+x_4X_4=0$$

给出. PG(3, p^n)中的直线可视为一对平面的交或等价地说成:
[284] 两点间的连线为满足

$$(\lambda a_1+\mu b_1, \lambda a_2+\mu b_2, \lambda a_3+\mu b_3, \lambda a_4+\mu b_4)\neq(0,0,0,0)$$

的点集,其中(a_1, a_2, a_3, a_4)和(b_1, b_2, b_3, b_4)为两个不同的点,而 λ,μ 遍历 GF(p^n)的元素.

作为一个例子,我们来考虑一个二进制射影空间 PG(3,2),它有 15 个点,也就是去掉(0,0,0,0)后的由 0 和 1 构成的四元序组集合. 它也有 15 个平面,每个平面都是一个含有 7 个点和 7 条线的 PG(2,2). PG(3,2)含有 35 条线,每条线由 2 个点组成,它们是按模 2 作加法运算. 事实上,PG(3,2)的点和线构成了 80 个 15 阶的施泰纳三元组(请与第 286 页作比较).

一个更好的用 15 个点表示 PG(3,2)的方法是:用具有 15 个非零元素的伽罗瓦域 GF(2^4)给出的. 这 15 个元素是关于 x 的模于 x^4+x+1 的 15 个多项式,其系数为 0 或 1(比较第 76 页). 由于 $x^4=x+1$,故所有的多项式都是 x 的幂,这能从下面的表示看出,其中每个多项式写为分离系数形式,所以 10011 = 0:

我们必须知道,而且我们必将知道

http://maths352.bokee.com



$$
\begin{array}{lcrrrrrrrl}
x^0 & = & & & & & & & 1 & = 0001, \\
x^1 & = & & & & & x & & & = 0010, \\
x^2 & = & & & x^2 & & & & & = 0100, \\
x^3 & = & x^3 & & & & & & & = 1000, \\
x^4 & = & & & & & x & + & 1 & = 0011, \\
x^5 & = & & & x^2 & + & x & & & = 0110, \\
x^6 & = & x^3 & + & x^2 & & & & & = 1100, \\
x^7 & = & x^3 & & & + & x & + & 1 & = 1011, \\
x^8 & = & & & x^2 & & & + & 1 & = 0101, \\
x^9 & = & x^3 & & & + & x & & & = 1010, \\
x^{10} & = & & & x^2 & + & x & + & 1 & = 0111, \\
x^{11} & = & x^3 & + & x^2 & + & x & & & = 1110, \\
x^{12} & = & x^3 & + & x^2 & + & x & + & 1 & = 1111, \\
x^{13} & = & x^3 & + & x^2 & & & + & 1 & = 1101, \\
x^{14} & = & x^3 & & & & & + & 1 & = 1001.
\end{array}
$$

这 15 个点中的任意两个决定一条直线，这两点相应的坐标相加所得到的点也落在该直线上. 例如，连接 x^4 和 x^5 的直线包 [285] 含有第三个点 $x^4+x^5=0011+0110=0101=x^8$. 或更直接地说，$x^4+x^5=x^4(1+x)=x^4x^4=x^8$. 因此，对 x 所作的乘法运算是以 15 为周期的把点映成点，线映成线，因此也把面映成面的一种直射变换(collineation). 很清楚，由这个直射变换所生成的循环群对 15 个点 x^0, x^1, …, x^{14}是可递的，但对 35 条线不是可递的. 这样就把 35 条线划分为三类子集，其中一类包含诸如$\{x^0,x^1,x^4\}$的 15 条(它由方程 $x^4+x+1=0$ 所生成)，另一类包含诸如 $\{x^0,x^2,x^8\}$ 的 15 条，还有一类包含诸如

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$\{x^0, x^5, x^{10}\}$的 5 条.这种划分①能用来解决后边由柯克曼所提出的女学生问题.

三维有限仿射空间 AG$(3, p^n)$可从 PG$(3, p^n)$中删去任一平面及该平面上的点和线而得到.因而,它的$(p^n)^3$ 个点可用 GF(p^n)中的三元序组给出.但我们还可以做得更好.例如,有 27 个点的三元仿射空间(ternary affine space)AG(3,3),就可用 GF(3^3)中的元素描述,也就是由 0 和 x 的 26 个乘幂来描述,这里的 x 是方程$x^3 = x - 1$ 的原根(primitive root).则按模 3 可知

$$x^{13} = x^4(x-1)^3 = x^4(x^3-1) = x^4(x+1) = x(x^2-1) = -1,$$

从而这 27 个点可由图 10.9 中的指数表出.

$$x^0 = 00+,\quad x^1 = 0+0,\quad x^2 = +00,\quad x^3 = 0+-,$$
$$x^4 = +-0, \cdots,\quad x^{13} = 00-, \cdots$$

[286] 并且把 x^∞定义为 $x^\infty = 000$.当然,若是三点之和为零,则其共线.例如$\{x^\infty, x^0, x^{13}\}$和$\{x^0, x^4, x^5\}$.用 x 相乘是保持原点固定不变的一个仿射,它把任一条线$\{x^\infty, x^i, x^{i+13}\}$及其 8 条平行线映到线$\{x^\infty, x^{i+1}, x^{i+14}\}$及其 8 条平行线上.因此,这个由仿射生成的循环群把 AG(3,3)的 117 条线划分为每九条平行线为一束的 13 束,即

(∞,3,16)	(0,1,22)	(4,6,12)	(7,10,21)	(11,18,2)
(∞,4,17)	(1,2,23)	(5,7,13)	(8,11,22)	(12,19,3)
(∞,5,18)	(2,3,24)	(6,8,14)	(9,12,23)	(13,20,4)
等等	等等	等等	等等	等等
(13,14,9)	(17,19,25)	(20,23,8)	(24,5,15)	
(14,15,10)	(18,20,0)	(21,24,9)	(25,6,16)	
(15,16,11)	(19,21,1)	(22,25,10)	(0,7,17)	
等等	等等	等等	等等	

类似地,n 维三元仿射几何AG$(n, 3)$可用GF(3^n)中的3^n

① J.Singer, Transactions of the American Mathematical Society, 1938, Vol. XLIII, pp.377—385.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

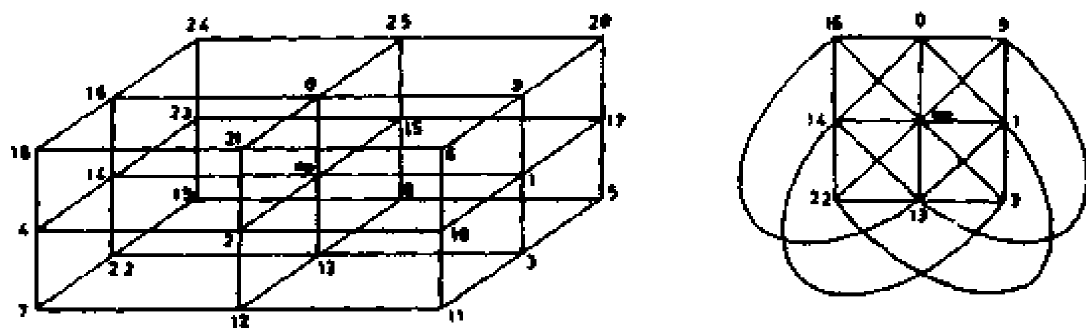


图 10.9

个元素描述．而 AG(n,3)中线的数目，通过排列三个超平面 $x_n=1, x_n=0, x_n=-1$ 上的点来计算，这三个超平面各有 3^{n-1}个点．从而可推出 $b_n=3^{2(n-1)}+3b_{n-1}$，因此 $b_n=\frac{1}{2}3^{n-1}(3^n-1)$．每条线有三个点，每个点落在$\frac{1}{2}(3^n-1)$条线上，并且每一对点都落在一条线上．因此，AG($n$,3)含有$\frac{1}{2}(3^n-1)$个平行线束．

柯克曼女学生问题　一位女校长有每天带着女学生散步的习惯．共有 15 个女生，每三位一行共排成五行．这样每个女孩都有两个同伴．问题是如何安排方能在连续七天中没有任何两人作伴的次数超过 1．更为一般的问题是：如何安排 n 个女生，此处 n 是 3 的奇数倍，在$\frac{1}{2}(n-1)$天里每三个一组出去散步，没有任何两人作伴次数超过 1．

按照这种方式提出的问题曾在本书第 10 章介绍过，所用标题一致．那一章写于 1892 年，后多次修改，考虑了几种答案和解法，但对一般的情况未能解决．实际上，问题的彻底解决到 1969 年才由 [287]
雷－钱杜瑞(D.K.Ray-Chaudhuri)和威尔森(R.M.Wilson)完成．

特殊情形下的 15 个女学生问题，柯克曼①先于施泰纳于

① T. Kirkman, Cambridge and Dublin Mathematical Journal, 1847, Vol. Ⅱ, pp.191—204.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

1847 年就提出来了. 而一般的情形则等价于求一个具有平行性的施泰纳三元组 $S(v)$，也就是对三元序组的集合作这样的一个划分，使得对任意的点 P 和任意的三元组 l，在含有 l 的部分中存在唯一的一个三元组，它包含 P 但不与 l 相交. 本例中，在 15 个女生所构成的三元组中只规定具有如下性质的 35 个三元组：要求每对女生在一个三元组中只出现一次，另外还要求在七天中的每一天，15 个女生应安排成五个三元组. 因此，35 个三元组应划分为每五个一类的七个平行类. 一般的女生问题便是求一个柯克曼系统，即一个带有平行性的施泰纳三元组，其参数为：$v=6t+3, b=(3t+1)(2t+1), r=3t+1, \lambda=1$.

雷－钱杜瑞和威尔森指出①：这个问题对每个非负整数 t 至少有一个解. 他们开发了一些合成定理（Composition Theorems），利用它们可以从低阶的设计来构造高阶的设计. 为此，要用到不等区组的区组设计和其他类型的组合设计. 此外，他们要构造许多这种低阶的设计，以便用合成定理把所有的阶数 $v\equiv 3 \pmod 6$ 都包括进去. 本书的前一版载明了对阶数为 $9\leqslant v\leqslant 99$ 的柯克曼系统的直接构造.

虽然柯克曼系统的存在性问题在 1969 年已经解决，但对于各种阶数 $v\equiv 3 \pmod 6$ 的情况，究竟有多少个不同的柯克曼系统仍待确定. 现在只知道对于 $v=9$ 实质上存在 1 个，对于 $v=$
[288] 15②，实质上存在 7 个.

下面我们就 $v=15$ 和 $v=27$ 给出一个解答. 回想（第 290 页）二进制射影空间 PG(3,2) 有 15 个点，它们可用 $GF(2^4)$ 中的

---

① D.K.Ray-Chaudhuri and R.M.Wilson, Proceedings Symposia Pure Mathematics, Combinatorics, 1971, Vol. LXX, pp.187—203.

② P. Mulder, Kirkman-Systemen (Groningen Dissertation, Leiden, 1917); F.N.Cole, Bulletin of the American Mathematical Society, 1922, Vol. XXVIII, pp.435—437.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

基本元素x的乘幂表示.用x乘后将35条线划分为三类,各类所包含直线的条数分别是5,15,15,即

$\{x^0,x^5,x^{10}\},\{x^1,x^6,x^{11}\},\{x^2,x^7,x^{12}\},\{x^3,x^8,x^{13}\},$

$\{x^4,x^9,x^{14}\}$;

$\{x^0,x^1,x^4\},\{x^1,x^2,x^5\},\{x^2,x^3,x^6\}$等;

$\{x^0,x^2,x^8\},\{x^1,x^3,x^9\},\{x^2,x^4,x^{10}\}$等.

如果用15个点代表15个女学生,35条线代表35排,我们找到每五条线一组的七个组,每组都包含了全部15个点.任何这样的一组,我们把它叫做一个*线展*(a spread of lines),它是由五条相互倾斜的直线构成,由于每条线都含有三个点.可以看出,第一类形成了一个线展,而第二、第三类都不包含一个线展.然而第二类却包含了四条互相倾斜的直线,其所以如此,是因为留下的三点不为这些直线所覆盖,而是落在了第三类的一条直线上.经过这番考察之后,便导出下面的解,其中用i代替x^i来表示女学生:

星期日	星期一	星期二	星期三	星期四	星期五	星期六
0,5,10	0,1,4	1,2,5	4,5,8	2,4,10	4,6,12	10,12,3
1,6,11	2,3,6	3,4,7	6,7,10	3,5,11	5,7,13	11,13,4
2,7,12	7,8,11	8,9,12	11,12,0	6,8,14	8,10,1	14,1,7
3,8,13	9,10,13	10,11,14	13,14,2	7,9,10	9,11,2	0,2,8
4,9,14	12,14,5	13,0,6	1,3,9	12,13,1	14,0,3	5,6,9

接着柯克曼的3^n个女学生问题,我们再考虑第293页的仿射几何AG$(n,3)$.把3^n个点当作女学生,而把$\frac{1}{2}3^{n-1}(3^n-1)$条线当作学生排成的行,我们要求$\frac{1}{2}(3^n-1)$个线族,每个线族含有$3^{n-1}$条线,并且包含了所有的点.一种方法是把所有直线划分成$\frac{1}{2}(3^n-1)$个平行线族.对于$n=3$的情况,在第292页已给

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[289] 出明显的解答.

拉丁方 回想第 195 页的 n 阶拉丁方,乃是一个 n 阶的方阵,它的每行每列都是 n 个字母的一个排列.两个 n 阶的拉丁方正交指的是:两个矩阵对应位置的元素所构成的 n^2 个序偶皆只出现一次.这是欧拉的定义.下面 4 阶的拉丁方中,前三个是两两正交的:

$$\begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & d & a & b \\ d & c & b & a \\ b & a & d & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & c & b & a \\ b & a & d & c \\ c & d & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ b & c & d & a \\ c & d & a & b \\ d & a & b & c \end{pmatrix}.$$

然而,第四个拉丁方是不可扩充的,没有和它正交的伙伴.

拉丁方以及相互正交的概念,在各种智力游戏、数学及应用中都很有意义.下面我列举五个例子,它们都涉及到 4 阶的拉丁方.

有 16 个女孩,每四人一组划分为四组,一天划分一次.要求在 x 天中,任两个女孩只有一次分在同一个组中,问应如何划分.例如,当 $x=3$ 时,可用 4 阶的拉丁方给出一个答案.我们把矩阵中的元素代表女孩.第一天,按照行来排,第二天按列来排,第三天按字母排.对于 $x=4$,用任一对正交的拉丁方都可给出一种解答,而至于 $x=5$,用三个两两互相正交的四阶拉丁方便可解决.

假定在农业试验中,我们打算比较四种不同小麦的产量.为了消除不可避免的土壤结构和肥沃程度的差异,试验田被划分为 4 行 4 列共 16 块.四种小麦按拉丁方进行种植,使得每种小麦种在每行每列的一块上,且只种一块.这样处理在作对比实验时,土壤结构及肥沃程度所产生的影响均等,差异可以消除.在
[290] 同一实验中,还可研究 4 种不同的施肥方法的效果,这只需借助与前一拉丁方正交的另一个拉丁方.这样每种不同的施肥方法都能在不同种类的小麦上实验一次.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

如果想比较 4 种型号的车胎的耐磨能力，显然要将它们装在一辆 4 轮轿车上. 但由于载荷不均，四个轮子上的磨损会有差异，因此需要调换位置再作实验；而先后时间的安排，会因当时气候条件的变化产生影响. 因而合适的实验方案应按拉丁方加以处理.

在任意两个相互正交的 4 阶拉丁方中，我们用同样字符的集合{1,2,3,4}代表行、列、拉丁字母和希腊字母. 那些正交的拉丁方可看成是由字符集{1,2,3,4}组成的 16 个有序四元组，并且每组字符恰好在每组坐标中出现一次. 这样，两个不同的四元组至少有三个不同的坐标. 因而便得到一种编码，共有 16 个码字，每个码字有 4 个坐标，共用 4 个字符集，最小距离为 3，故为纠 1 码.

我们最后的一个例子是关于电视荧屏的实验. 有 $n\times n$ 个方格单元要按 n 种不同灰度进行着色，这样便能在竖直和水平方向按成对的邻接次序形成反差. 下面是对 $n=4$ 和 $n=6$ 两种情况所采用的拉丁方：

$$\begin{pmatrix} a & b & c & d \\ c & a & d & b \\ b & d & a & c \\ d & c & b & a \end{pmatrix},\quad \begin{pmatrix} a & b & c & d & e & f \\ b & d & f & a & c & e \\ c & f & b & e & a & d \\ d & a & e & b & f & c \\ e & c & a & f & d & b \\ f & e & d & c & b & a \end{pmatrix}.$$

这些例子都是为帮助理解拉丁方的概念而提出的. 实际上，在某些情况下，行、列和字母的特殊作用是不相关的. 我们所用的仅仅是“从 n 个字符的集合确定出 n^2 个有序的三元组，使得对每对坐标，每对字符只出现一次”这一性质. 如果把这一性质当作定义，则对 n 阶的拉丁方的数目，可算出： [291]

n	2	3	4	5	6	7	8
m	1	1	2	2	12	147	>250 000

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

按原来关于拉丁方的定义，4 阶的拉丁方有 110 592 个．但若允许行、列和字母的置换以及行、列的交换，则数目等于 4．而在新的定义之下，数目等于 2，并把这两种类型分别表示为可扩展的拉丁方和不可扩展的拉丁方．

这个新定义也可以用于正交的拉丁方．一组 $k-2$ 个两两正交的 n 阶拉丁方便可看作是 n 个符号所构成的一组 n^2 个有序 k 元序组，且在它们的每对坐标中，每对符号只出现一次．因而任何一对 k 元序组有一个或者没有公共坐标．

正如在第 198 页指出的，欧拉在 1782 年的猜想：没有一对互相正交的 $n=4k+2$ 阶的拉丁方．塔里曾就 $n=6$ 证明了这个猜想，而玻色(R. C. Bose)，帕克(E. T. Parker)，和施瑞克罕德①(S. S. Shrikhand)证明了这个猜想并非对所有的 $n=4k+2$，$k>1$，都成立．读者要知道：这个猜想持续了 177 年之久，但只对一种情况是成立的，而对于其他的情况都是错误的．一旦认识到这点，很容易给出二个 $n=10$ 阶的正交拉丁方的例子，然后可立即推广到 $n=3m+1$：

0	6	5	4	7	8	9	1	2	3
9	1	0	6	5	7	8	2	3	4
8	9	2	1	0	6	7	3	4	5
7	8	9	3	2	1	0	4	5	6
1	7	8	9	4	3	2	5	6	0
3	2	7	8	9	5	4	6	0	1
5	4	3	7	8	9	6	0	1	2
2	3	4	5	6	0	1	7	8	9
4	5	6	0	1	2	3	9	7	8
6	0	1	2	3	4	5	8	9	7

0	9	8	7	1	3	5	2	4	6
6	1	9	8	7	2	4	3	5	0
5	0	2	9	8	7	3	4	6	1
4	6	1	3	9	8	7	5	0	2
7	5	0	2	4	9	8	6	1	3
8	7	6	1	3	5	9	0	2	4
9	8	7	0	2	4	6	1	3	5
1	2	3	4	5	6	0	7	8	9
2	3	4	5	6	0	1	8	9	7
3	4	5	6	0	1	2	9	7	8

[292]

上表分块记为：

① R. C. Bose, S. S. Shrikhand, and E. T. Parker, Canadian Journal of Mathematics, 1960, Vol. Ⅻ, pp. 189—203. The frontispiece shows a modified version.

我们必须知道，而且我们必将知道

A	B
C	D

A^T	C^T
B^T	E

我们对 $n=3m+1$(在上面例子中 $m=3$)解释一下它的结构①:A 的主对角元包含字符 $0,1,2,\cdots,2m$;其余的与主对角线平行的 $2m$ 条中有一半是由相同的符号组成,只不过进行了移位,分别以 $2m,2m-1,\cdots,m+1$ 开头;余下的另一半平行线,是由相同元素组成,分别是 $2m+1,2m+2,\cdots,3m$. B 中的列(或 C 中的行)是从$(1,2,\cdots,m)$开始的按一定顺序循环生成的. D 和 E 是符号 $2m+1,2m+2,\cdots,3m$ 的两个互相正交的拉丁方.除了 E 之外,第二个表中的三块可从第一个表中的三个作转置得到.在 $m=3$ 的情况下,把 10 分成 7+3 两块,会误认为欧拉方能以一种较为对称的形式出现.

欧拉猜想的错误在 1922 年又在麦克尼希(MacNeish)身上重演,他构造了 t 个 n 阶的相互正交的拉丁方,此外 t 是小于 n 的素数分解中最小素数的幂.麦克尼希进一步猜想:对于 n,至多有 t 个这样的方形存在.因此,在这一猜想之下,对 $n=4k+2=2(2k+1)$不存在欧拉方.然而,帕克在 1959 年利用射影平面 PG$(2,2^2)$构造出三个 21 阶的相互正交的拉丁方,从而否定了麦克尼希的猜想.此后,玻色和施瑞克罕德借助于推广了的区组设计,利用不等区组构造了五个 50 阶的相互正交的拉丁方,从而否定了欧拉猜想.利用修改了的柯克曼系统,他们还构造出 22 阶的欧拉方.然后帕克找到了 10 阶的 [293]
欧拉方.在嗣后的几周里,这三位数学家解决了所有其他的情况,得到以上的结论.

欧拉猜想被推翻的消息成为当年世界舆论的头条新闻,

① P.Kesava Menon, Sankhya, 1961, Vol.A XXIII, pp.281—282.

http://maths352.bokee.com

1959 年 4 月 26 日的“纽约时报”刊载了详细的报道和照片.虽然图片中只能见到一部分欧拉方,而很多学生都没法补出其余的部分.

下面我们通过构造与他们的转置正交的拉丁方来结束本节.令 GF(q)是任一伽罗瓦域,$q \neq 2,3$(例如,以大于 3 的素数为模的剩余类).令 λ 是 GF(q)中的一个固定元,且 $\lambda \neq 0,1,\frac{1}{2}$.考虑矩阵

$$[\lambda a+(1-\lambda)b],$$

其中的 a,b 取遍 GF(q).根据假设,没有一行和一列有两次含有域中的一个元.因此我们得到一个拉丁方.这个矩阵和其转置

$$[\lambda b+(1-\lambda)a]$$

形成了一个欧拉方.事实上,$\lambda a+(1-\lambda)b=\lambda c+(1-\lambda)d$ 和 $\lambda b+(1-\lambda)a=\lambda d+(1-\lambda)c$ 蕴含着 $a+b=c+d$,代入后便得

$$(1-2\lambda)b=(1-2\lambda)d,$$

因而 $b=d$, $a=c$.根据标准的方法,这种构造可以推广到任意的阶数 n,但 n 的素数分解不含有 2 或 3 的一次幂.下面在 GF(2^3)的基础上给出一个例子:

$$\begin{pmatrix} 0 & 3 & 5 & 6 & 7 & 1 & 4 & 2 \\ 2 & 1 & 4 & 7 & 6 & 3 & 5 & 0 \\ 4 & 7 & 2 & 1 & 3 & 6 & 0 & 5 \\ 5 & 6 & 0 & 3 & 1 & 7 & 2 & 4 \\ 3 & 0 & 6 & 5 & 4 & 2 & 7 & 1 \\ 7 & 4 & 1 & 2 & 0 & 5 & 3 & 6 \\ 1 & 2 & 7 & 4 & 5 & 0 & 6 & 3 \\ 6 & 5 & 3 & 0 & 2 & 4 & 1 & 7 \end{pmatrix}.$$

[294]

正方体和单形 在下面的几节,取三维空间中通常的正方体(见图 10.10)作为我们研究的起点.其顶点的坐标我们有时用 0 和 1 表示(原点为 O,边长为 1),有时用 $+1$ 和 -1 表示(原点为

我们必须知道，而且我们必将知道

http://maths352.bokee.com

O，边长为 2）. 如图 10.10 中第三个图形所示，它是由 8 个顶点和 12 条棱构成的集合，同一条棱的两端的顶点只有一个坐标不同.

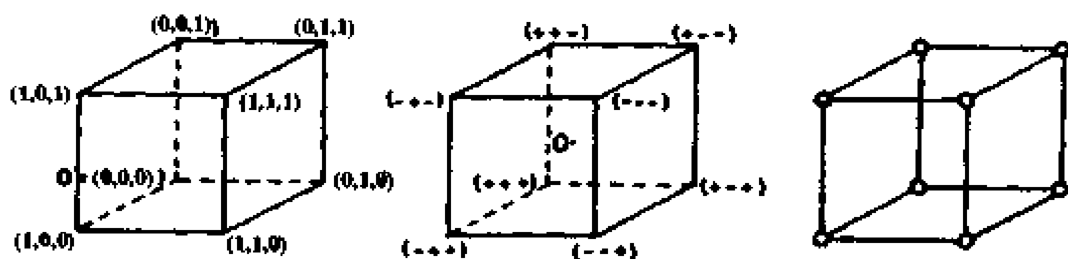


图 10.10

n 维立方体在 n 维空间中有 2^n 个顶点，即坐标如 $(x_1, x_2, \cdots, x_n)$ 的点构成的集合 V，其中 x_i 等于 0 或 1. V 中每对仅有一个坐标不同的点偶连成一棱，便构成棱的集合.

n 维空间中的 n 维单形是这样一个多面体：它有 $n+1$ 个顶点，两两之间的距离相等. 它是正三角形（$n=2$）和正四面体（$n=3$）的推广. n 维单形也可用 $(n+1)$ 元组 $(1,0,\cdots,0)$，$(0,1,0,\cdots,0)$，$\cdots$，$(0,0,\cdots,0,1)$ 来定义，也就是 $(n+1)$ 维空间中的 $n+1$ 个点，它们落在 n 维子空间 $x_1+x_2+\cdots+x_{n+1}=1$ 中（见图 10.11 中的最后一个）.

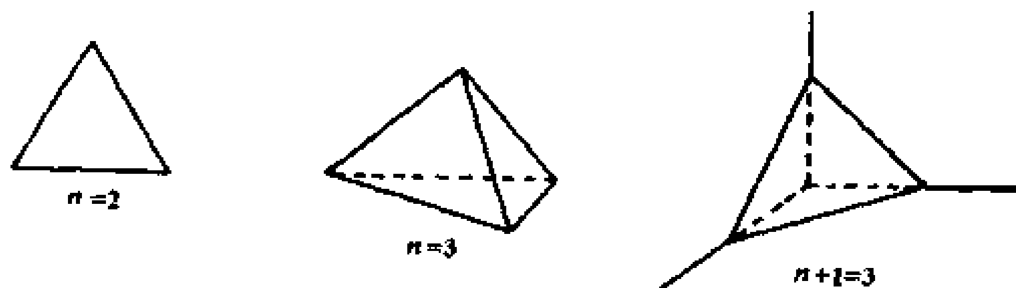


图 10.11 [295]

阿达玛矩阵 在三维空间中给定有 8 个顶点的立方体（如图 10.10 的第二个），问能否从 8 个顶点中选取 4 个以构成一个正四面体？回答是肯定的，取下面四个顶点：

$$(+\ +\ +),(+\ -\ -),(-\ +\ -),(-\ -\ +).$$

我们必须知道，而且我们必将知道

http://maths352.bokee.com

其边长为$\sqrt{3}$,每对的内积为-1(见第138页).每一点增加一个常值坐标$x_0=+1$,便得到矩阵

$$H_4=\begin{pmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{pmatrix},$$

它的每两行的内积为0.因此H_4是一个4阶的阿达玛矩阵.在第278页我们曾构造过一个8阶的阿达玛矩阵,在第308页我们将构造一个12阶的阿达玛矩阵.

阿达玛矩阵H_r是一个r阶的方阵,其元素是$+1$和-1,它的每两行都是正交的:

$$H_rH_r^T=rI.$$

构造r阶的阿达玛矩阵H_r等价于①在$r-1$维空间中从有2^{r-1}个顶点的超正方体中选取r个顶点构成一个$r-1$维单形.对于$r=3$显然是做不到的.事实上,H_r存在的必要条件是:

$$r=2\text{ 或 }r=4s,\quad s\text{ 是一个正整数}.$$

人们曾猜想这个必要条件也是充分的.对于$r<188$和另外的无穷多个r的值,证明了这一猜想.西尔维斯特曾迭代地构造了下
[296] 面$2^t(t=1,2,3,\cdots)$阶的阿达玛矩阵序列:

$$H_2=\begin{pmatrix} + & + \\ + & - \end{pmatrix},H_4=\begin{pmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{pmatrix},H_8=\begin{pmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{pmatrix},\cdots$$

上面所构造的H_4与从正方体构造的H_4一致.在第278页所构造的阿达玛矩阵经过适当的排列,与这里的H_8相同.

从迭代构造的H_{32},我们又可得到一个32×64阶的矩阵

$$[H_{32},-H_{32}].$$

让我们再回到第275页,在那里我们曾考虑过$r=8$的情形,可

① H.S.M.Coxeter, Journal of Mathematics and Physics, 1933, Vol. Ⅶ, pp.334—345.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

以看出这个矩阵的列形成了一个纠 7 的线性码(32,6).1969 年 3 月,"水手－1969"号宇宙飞船朝着火星发射,五个月后收到了火星的照片.而"水手－1969"号上的高速遥测系统所使用的码制就是基于上面所说的(32,6)码①.

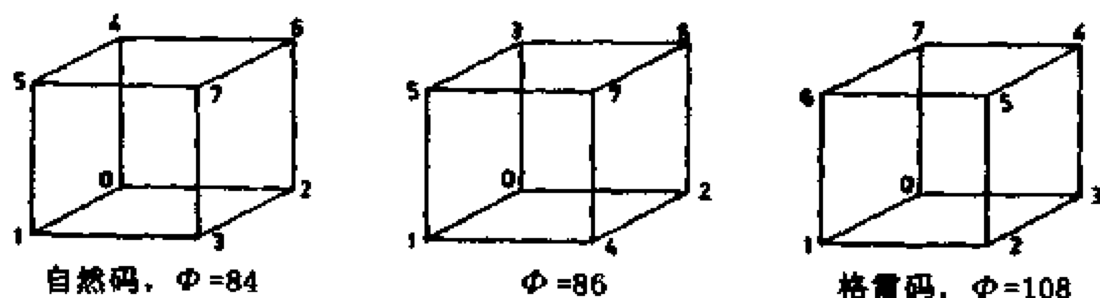
图象传送 设 n 维正方体的顶点的集合为 V 而棱的集合为 E,并用整数 $0,1,2,\cdots,2^n-1$ 分别一对一地指配给各个顶点:

$$\phi: V \leftrightarrow \{0,1,2,\cdots,2^n-1\}.$$

则对于 $n=3$,有 $(2^n)!=40320$ 种可能的指配方案.其中的三种方案在图 10.12 中给出.我们感兴趣的是,这些 ϕ 中的哪一个使

$$\Phi = \sum_{(v,w)\in E}[\phi(v)-\phi(w)]^2$$

取最小值.



自然码, $\Phi=84$　　　$\Phi=86$　　　格雷码, $\Phi=108$

图 10.12 [297]

在这个例子中,$\Phi=84,86,108$,因此第一种分配方案在给定的三种方案中最佳.我们将要证明,对于 $n=3$,不必计算所有 40 320种方案对应的 Φ 值,第一种方案也是最佳的.

我们约定,根据顶点 v 的坐标中所包含 1 的个数的奇偶性,而把它叫做奇顶点或偶顶点.并把 v^c 叫做与 v 相反的顶点,也就是顶点集合 V 中的这种点:它的每个坐标分量与 v 的对应的

① Edward C. Posner, "Combinatorial Structures in Planetary Reconnaissance," in H.B.Mann, Error Correcting Code, New York, 1968; see fig, Ⅲ on p.23.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

分量相反，例如$(0,1,0)^c=(1,0,1)$．则对于 $n=3$，我们有

$$\sum_{(v,w)\in E}[\phi(v)-\phi(w)]^2=3\sum_{v\in V}\phi^2(v)-2\sum_{(v,w)\in E}\phi(v)\phi(w)$$
$$=3\sum_{v\in V}\phi^2(v)-2\sum_{v奇}\phi(v)\sum_{w偶}\phi(w)+2\sum_{v,v^c\in V}\phi(v)\phi(v^c).$$

第一项与 ϕ 无关；对于第二项，如果

$$\sum_{v奇}\phi(v)=\sum_{w偶}\phi(w)=14,$$

则由于

$$\sum_{v\in V}\phi(v)=0+1+\cdots+7=28,$$

可知它取最大值；同样的道理，最后一项中的被加数为 0×7，1×6，2×5，3×4 时，它取最小值．由下式

$$\phi(v)=\sum_{i=0}^{n-1}v_i2^i$$

所定义的 ϕ，很容易看出满足这些条件，所以 Φ 达到极小．由于式

$$\sum_{v奇}\phi(v)=n_1+n_2+n_3+7=14,\quad 1\leqslant n_1<n_2<n_3\leqslant6$$

的唯一解是 $n_1=1,n_2=2,n_3=4$，因此我们的 ϕ 是唯一的．因而所得到的解是自然解(natural solution)：它赋予每个顶点的整数的坐标构成了二进制展开式．

这个数学问题有其实际的应用．在工程技术中，区间长度为
[298] n 且具有单一的误差概率较小的二进制对称通道结构，便可用 n 维立方图来近似表示．假如有数据点 $0,1,\cdots,2^n-1$ 要传送，例如一个图象中的有 2^n 种不同亮度的点．那么赋值 ϕ 便是一个码，并且

$$\sum_{(v,w)\in E}[\phi(v)-\phi(w)]^2$$

与噪声能量成正比，显然我们希望将它极小化．我们知道，自然码和格雷码(Gray code)都能使平均绝对误差达到最小；但自然码能使噪声能量达到极小，而格雷码却使其达到最大．这里的平均绝对误差指的是

$$\sum_{(v,w)\in E}|\phi(v)-\phi(w)|.$$

因此，用格雷码传送使误差的主效应更为突出．对任意的 n，最

我们必须知道，而且我们必将知道

http://maths352.bokee.com

近又给出了更为一般的解决①.

三维空间中的等角线　让我们再看看以 O 为中心的正方体 $(ADBC)(B'C'A'D')$，见图 10.13. 向量 OA、OB、OC、OD 之间的夹角的余弦分别是

$$\cos AOD = \cos DOB = \cos BOC = \cos COA = \frac{1}{3},$$

$$\cos AOB = \cos COD = -\frac{1}{3},$$

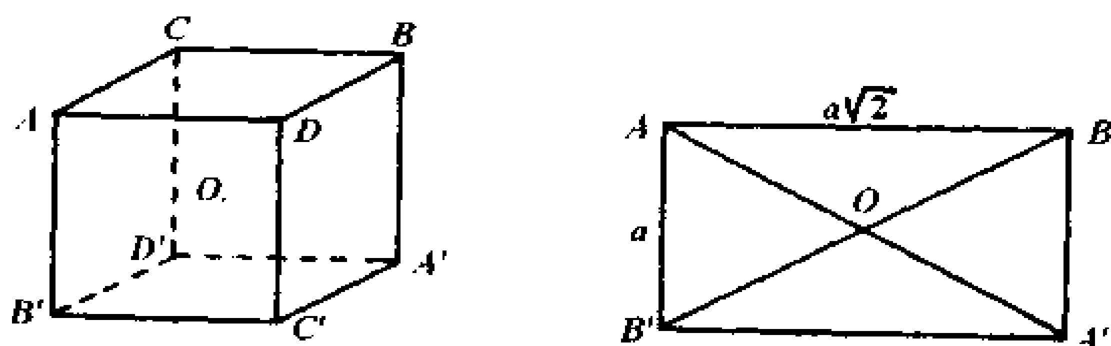


图 10.13 [299]

只要考虑一个对角平面便可验证之. 这个立方体的四条对角线 AA', BB', CC', DD'，两两之间的夹角相等，这里的夹角指的是两线所形成的两个互补角中较小的一个. 如果一族直线中的每两条的夹角都相等，则把该线族叫做等角的，我们已找到了一族包含四条线的等角线族.

我们还能得到更大的等角线族. 事实上，连接正二十面体的每两个对极点所得到的六条直线：AA', BB', CC', DD', EE', FF'，根据初等的对称性论证，便知它们也构成一个等角线族，见图 10.14. 可以证明，在三维空间中等角线族的最高阶数是 6，并且上面给出的一族是唯一的. 再者，如果从中删去任一条对角

① IEEE Transactions, Information Theory, 1969, Vol. IT - 15, pp.72—78.

我们必须知道，而且我们必将知道

线，便得到一个 5 阶的等角线族. 然而，有两种不同的 4 阶等角线族，一种可由正二十面体中删去任两条对角线得到，另一种像上面做的那样，从正方体中得到①.

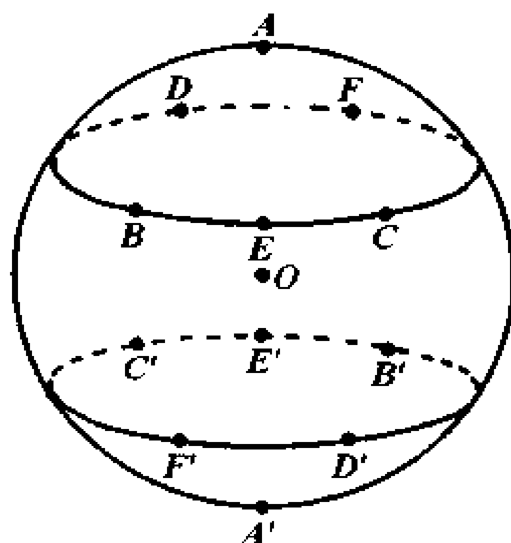


图 10.14

无论从正方体得到的 4 阶等角线族，还是从正二十面体
[300] 得到的 6 阶等角线族，我们从 O 点到点 $A, B, C, \cdots$ 沿直线方向取单位向量 $p_1, p_2, p_3, \cdots$，由于这些单位向量的内积都满足 $|p_i \cdot p_j| = \cos\phi$，其中 ϕ 是两线间的夹角，这些内积构成的矩阵 P 为：

$$P = [(p_i \cdot p_j)] = \begin{pmatrix} 1 & & & & & \pm\cos\phi \\ & 1 & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & \cdot \\ \pm\cos\phi & & & & & 1 \end{pmatrix}.$$

① 这两种等角线族中的直线平行于两类十二菱面体的棱，这两类十二菱面体是：经典的一类和 Bilinski 的一类(见第 143 页).

http://maths352.bokee.com

从 P 减去单位阵 I，再除以 $\cos\phi$，便得到矩阵

$$A=[P-I]\sec\phi,$$

对于我们前面给出的例子，便是

$$A_4=\begin{pmatrix}0&-&+&+\\-&0&+&+\\+&+&0&-\\+&+&-&0\end{pmatrix},\quad A_6=\begin{pmatrix}0&+&+&+&+&+\\+&0&-&+&+&-\\+&-&0&-&+&+\\+&+&-&0&-&+\\+&+&+&-&0&-\\+&-&+&+&-&0\end{pmatrix}.$$

这些矩阵表明了：在 $OA,OB,OC,\cdots$ 中哪些向量对之间的夹角为锐角(余弦为正)，哪些为钝角(余弦为负)．每个这样的矩阵都可以看作为一个图的邻接矩阵：顶点 $A,B,C,\cdots$ 中任一对，如果它们所对应的矩阵元为 -1，则认为是相邻的，否则便认为是不邻接的(见图 10.15)．这些矩阵及相应的图为我们进一步的讨论提供了基础．稍作验算，便可看出矩阵 A_4 和 A_6 满足

$$(A_4-I)(A_4+3I)=0,\quad A_4J=J;\quad A_6^2=5I.$$

因此 A_6 是一个正交阵，它的任意两行的内积为 0．我们要注意这个结论的下述三个结果．

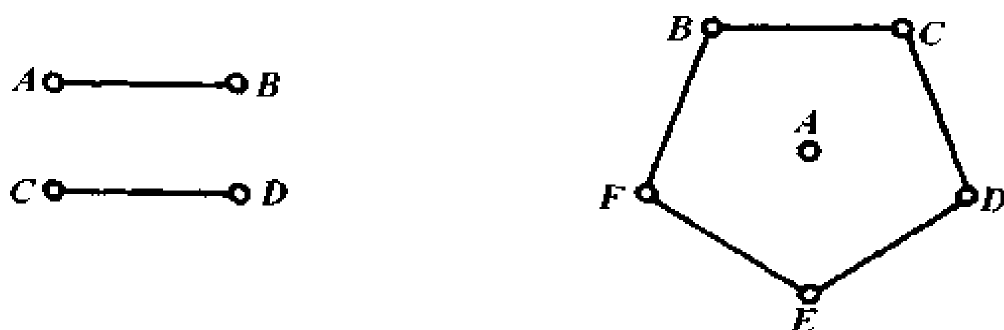


图 10.15 [301]

首先，A_6 的最小特征值是 $-\sqrt{5}$，而相应的 P_6 是一个秩为 3 的非负定矩阵，正二十面体的对角线之间的夹角 ϕ 满足 $-\sec\phi=-\sqrt{5}$，因此 $\cos\phi=\frac{1}{\sqrt{5}}$．其次，矩阵

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$$H_{12}=\begin{pmatrix}A_6+I_6 & A_6-I_6\\ A_6-I_6 & -A_6-I_6\end{pmatrix}$$

是一个 12 阶的阿达玛矩阵.

关于第三个应用①,就是 6×12 阶的矩阵

$$[A_6,\quad I_6],$$

它的 12 个列向量 $c_1,c_2,\cdots,c_{12}$看作为 GF(3)上的 6 维向量.通过观察可以知道,这些向量中的任何五个都是无关的,也就是说,从{0,1,-1}中取出的使得 $\alpha_1c_1+\alpha_2c_2+\cdots+\alpha_{12}c_{12}=0$ 成立的任一组数$\{\alpha_1,\alpha_2,\cdots,\alpha_{12}\}$,至少有六个不等于 0.这样的数组容易给出;只要取矩阵$[I_6,-A_6]$的 6 行和这些行的所有 3^6 个线性组合就行了.这一个 GF(3)上的 12 维向量空间的 6 维子空间(用类似于第 280 页的术语来说)是一个线性(12,6)三元 [302] 码.由于这些向量之间的距离都$\geqslant 6$,所以该码是纠 2 检 3 码.如果删去任一坐标,便得到最小距离为 5 的(11,6)码.因此,在这 11 维三元向量空间的 6 维子空间中以任意两个矢量为中心,2 为半径所作的球是不相交的.由于在整个空间中共有 3^{11}个向量,而在该子空间中共有 3^6 个向量,在每个球中有 $1+22+220$ 个矢量,所以这些球填满了整个空间.因此线性(11,6)三元纠 2 码是一种完备码.这种码是由戈莱②(M.Golay)发现的,进而还有线性(23,12)二元纠 3 的完备码.它们提供了这些能纠正多于一个错误的码制③.

① R.C.Bose, Bulletin de l'Institut International de Statistique, 1961, Vol. XXXVIII, pp.257—271.

② M.Golay, Proceedings of the Institute of Radio Engineers, 1949, Vol. XXXVII, p.637.

③ E.R.Berlekamp, Algebraic Codiong Theory, New York, 1968; J. H.von Lint, Coding theory, Lecture Notes in Mathematics 201, Springer, Berlin, 1971.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

高维空间中的直线 现在我们对高维空间做一探讨. 在 7 维空间中存在哪些等角线族? 通过考查 7 维单形便可获得一种答案, 它的 8 个顶点可用 8 维空间中的 8 个向量

$$(8,0,0,\cdots,0),(0,8,0,\cdots,0),\cdots$$

来表示. 8 维空间中方程为 $x_1+x_2+\cdots+x_8=8$ 的超平面通过这 8 个顶点, 经过平移与 $x_1+x_2+\cdots+x_8=0$ 重合. 这时上述的 8 个向量变成

$$(7,-1,-1,\cdots,-1),(-1,7,-1,\cdots-1),\cdots$$

而上述 7 维单形的各棱的共 28 个中点 $P_{h,i}(h<i,h,i=1,2,\cdots,8)$ 变成

$$P_{1,2}=(3,3,-1,-1,-1,-1,-1,-1),$$
$$P_{1,3}=(3,-1,3,-1,-1,-1,-1,-1),$$
$$P_{3,4}=(-1,-1,3,3,-1,-1,-1,-1),\cdots$$

这样, 连接原点 O 与中点 $P_{h,i}$ 的 28 条直线就构成了一个等角 [303]
线族, 其中 $\cos\phi=\frac{1}{3}$. 事实上, 向量 $OP_{h,i}$ 的长度为 $\sqrt{24}$, 两两的内积为 ± 8. 若向量 $OP_{h,i}$ 与 $OP_{j,k}$ 的标号偶有一个共同的数目,

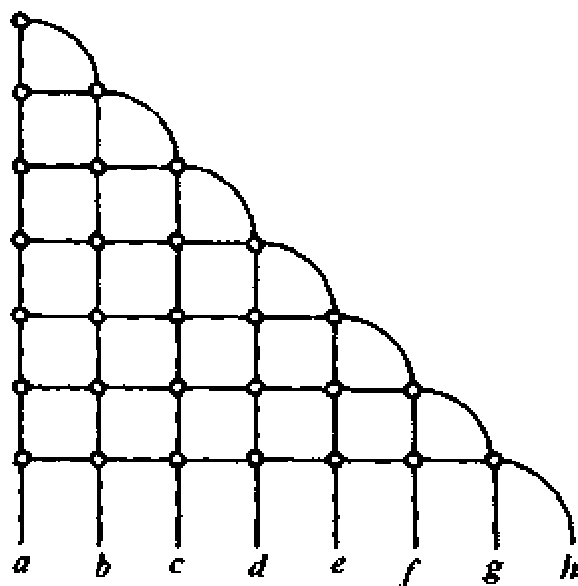


图 10.16 关于符号 $\{a,b,c,d,e,f,g,h\}$ 的 $T(8)$ 图

我们必须知道，而且我们必将知道

http://maths352.bokee.com

则其夹角为锐角，若没有共同的数目，则为钝角. 按第 307 页的规定，属于这一构形的图是三角形图 $T(8)$（见图 10.16）的补. 对于 $n>3$，n 阶的三角形图 $T(n)$ 是由 n 个符号构成的 $\frac{1}{2}n(n-1)$ 个无序偶组成，任意两个无序偶当且仅当它们有一个共同的符号时是邻接的. 譬如，在 $T(8)$ 中，顶点 ab 与包含 a 或 b 的 12 个顶点 ij 邻接.

在 7 维空间中我们构造了含有 28 条直线的等角线族① $\{P_{h,i}, h<i; h,i=1,2,\cdots,8\}$. 现在来看 6 维空间的情形. 集合 $\{P_{h,i}\}$ 的满足方程

[304] $$x_1+x_2+\cdots+x_8=0, \quad x_1=x_2$$

的一个子集，它包含 16 个点 $P_{1,2}$ 和 $P_{j,k}(j<k, j,k=3,\cdots,8)$. 原点和这些点的连线张成一个 6 维空间，并且构成一个含 16 条线的等角线族，其夹角满足 $\cos\phi=\frac{1}{3}$. 其实，还有更为简单的方法构成这个线族. 为此，让我们考虑曾在第 301 页用过的三维向量集合 S：

$$(+\ +\ +),(+\ -\ -),(-\ +\ -),(-\ -\ +).$$

在 6 维空间中取这样的 16 个向量，它们的前三个坐标和后三个坐标都取遍 S，并且两两的内积为 ± 2，这就提供了我们所要求的集合. 这 16 条等角线的构形图是格形图 $L(4)$（见图 10.17）的补. n 阶的格形图 $L(n)(n>1)$ 是由 n 个字符组成的 n^2 个序偶，任意两个序偶，当且仅当它们有一个共同的字符时，才定义为是邻接的. 譬如，在 $L(4)$ 中顶点 (a,a) 与下面 6 个顶点是邻接的：$(a,b),(a,c),(a,d),(b,a),(c,a),(d,a)$.

---

① 这些线连接了多胞形 3_{21} 的对顶点；见 H.S.M. Coxeter, Regular Polytopes, 3rd edition, New York, 1973, P.203. 也见 Proceedings of the Cambridge Philosophical Society, 1928, Vol. XXIV, pp.1—9.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

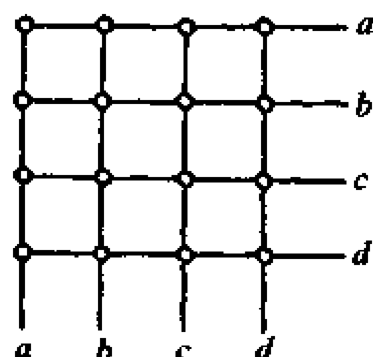
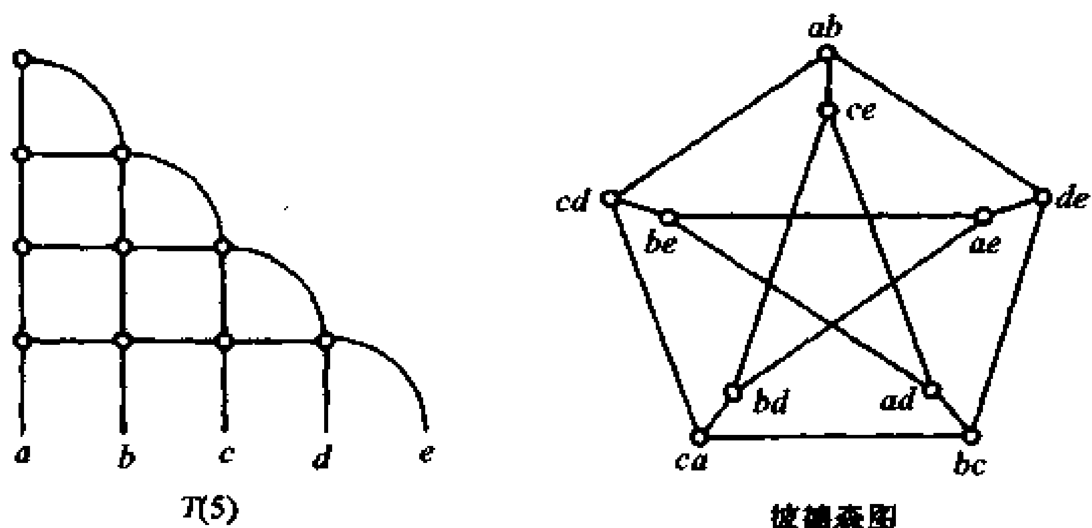


图 10.17 关于字符$\{a,b,c,d\}$的$L(4)$图

让我们回到 5 维空间，考查 28 个点构成的集合$\{P_{h,i}\}$的满足$x_1=x_2=x_3$的一个子集，它是由 10 个点 $P_{j,k}(j<k;j,k=4,5,\cdots,8)$组成，并且导出了 5 维空间中含有 10 条线的等角线族，其夹角满足 $\cos\phi=\frac{1}{3}$. 它的构形图是三角形图 $T(5)$的补，又叫做彼德森(A.C.Petersen)图（见图 10.18，也见第 230 页）．这些图与德沙格构形(Desargues configuration)密切相关（见图 10.19)．这种构形可用 10 个点和 10 条线来定义，它们按下列方式 [305] 位于一个平面上．三角形 ac,ad,ae 和 bc,bd,be 是以 ab 为中心的透视，它们的边相交于共线点 cd,de,ce．这一构形也可看作为三维空间中5个平面a,b,c,d,e的交（我们把交中的每



$T(5)$ 彼德森图

图 10.18

我们必须知道，而且我们必将知道

http://maths352.bokee.com

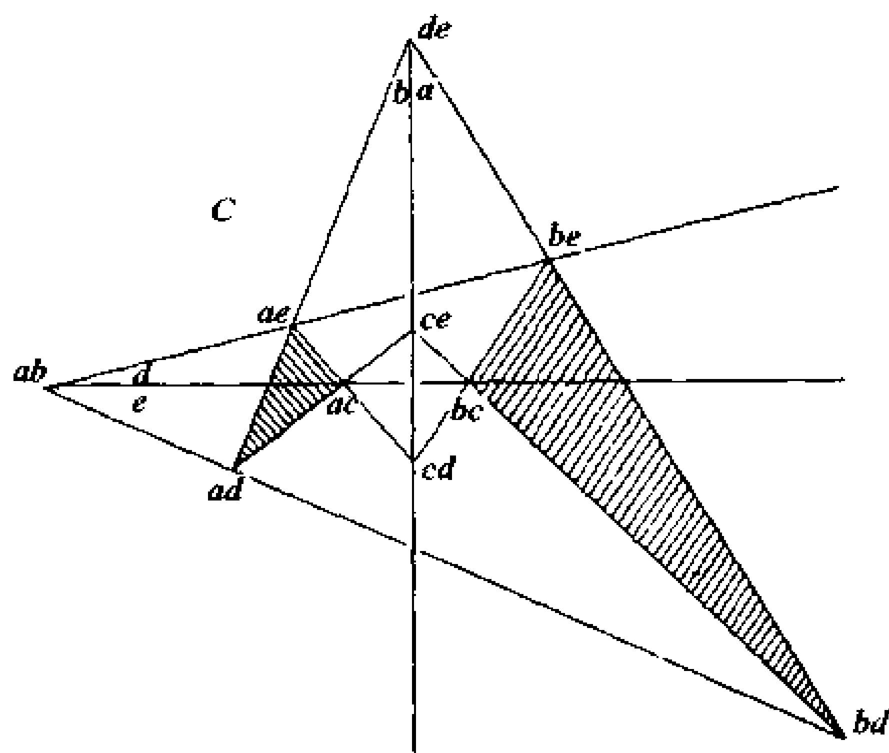


图 10.19 德沙格构形

[306] 个点用不过该点的一对平面来表示).

如果把德沙格构形中的落在同一条线上的两点叫做是邻接点的话,则该构形便成为三角形图,反之,为彼德森图.



图 10.20

为了从 28 点组$\{P_{h,j}\}$导出四维空间和三维空间中的等角线族,我们分别置 $x_1 = x_2 = x_3 = x_4$ 和 $x_1 = x_2 = x_3 = x_4 = x_5$. 前者给出了四维空间中含有 6 条线的等角线族,它的图是 $T(4)$的补,也就是一个三步梯状图(见图 10.20). 后者给出了 3 维空间中含有 4 条线的等角线族,其图是 $L(2)$的补,也就是一个二步梯状图(见图 10.21),这又使我们回想起在第 306 页开始时所

我们必须知道，而且我们必将知道

http://maths352.bokee.com

提到的立方体的四条对角线.



图 10.21

在下述意义下,上面所给出的例子是最优的.令 $v(n)$是 n 维空间中等角线的最大数目,则已经知道①:$v(2)=3$,$v(3)=v(4)=6$,$v(5)=10$,$v(6)=16$,$v(7)=28$,$v(15)=36$,$v(22)=176$,$v(23)=276$.在 7 维空间中,满足 $\cos\phi=\frac{1}{3}$的含有 28 条线的等角线族是不可扩充的.

另一方面,的确存在这样的线族,其夹角之一为 $\arccos\frac{1}{3}$.所以,在 24 维空间中存在包含 2 048 条线的"两角"族,夹角分别满足 $\cos\phi=\frac{1}{3}$和 $\cos\psi=0$.这种线族与第 308 页所提到的完备的戈莱(23,12)码密切相关.另外,这种线族与 24 维空间的一个球体密装有关.24 维空间的一个更为紧密的球装②对应于 [307]
由 98 280 条线组成的"三角"族,夹角分别满足 $\cos\phi=\frac{1}{4}$,$\cos\psi=\frac{1}{2}$,$\cos\chi=0$.它是这个线族的一个自同构群,在有限单群的理论中③,自同构群扮演着重要的角色.

---

① J.H.Van Lint and J.J.Seidel, Koninklijke Nederlandsche Akademie van Wetenshappen te Amsterdam, Proceedings, 1966, Vol.A.LXIX, pp.335—348.

② J.Leech, Canadian Journal of Mathematics, 1967, Vol.LXX, pp.251—267.

③ J.H.Conway, Proceedings of the National Academy of Science (U.S.A), 1968, Vol.LXI, pp.398—400.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

C 矩阵

$$C_6=\begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & + & - & - & + \\ + & + & 0 & + & - & - \\ + & - & + & 0 & + & - \\ + & - & - & + & 0 & + \\ + & + & - & - & + & 0 \end{pmatrix},\ C_4=\begin{pmatrix} 0 & + & + & + \\ - & 0 & - & + \\ - & + & 0 & - \\ - & - & + & 0 \end{pmatrix}.$$

上面两个矩阵都是 C 矩阵的例子，其中第一个与第 306 页的正二十面体的图相像. 由于这两个矩阵的任两行的内积都为零，所以都是正交的. 凡是对角元为 0，其余元为 ± 1 的且满足等式

$$CC^T=(v-1)I$$

的 v 阶对称或反对称阵，都叫做 C 矩阵. 下面给出这种矩阵的两个应用.

一家公司的 v 位董事要召开一次电话会议，会上每位董事都能与另一位董事对讲，且其余的董事也能随着参加讨论. 构造这样的一个(线性的，无漏失的，有 v 个往反通道的，与频率无关的，分布均匀的，零反射的)会议网络等价于构造一个对称的 C 矩阵*.

要称 v 个重物，共称 v 次(在一定的条件下，按某个"最佳"的定义)，哪种称法最佳？这个量称的策略可用矩阵 $C=(c_{ij})$来描述：

$c_{ij}=1$，若第 i 次称的第 j 个物体在天平左边；

$c_{ij}=-1$，若第 i 次称的第 j 个物体在天平右边；

[308] $c_{ij}=0$，若第 i 次没称第 j 个物体.

对于 $v\equiv 0(\text{mod}4)$，最佳量称设计可用阿达玛矩阵给出. 对于 $v\equiv 2(\text{mod}4)$，可用一个对称的 C 矩阵给出①.

① D. Raghavarao, Constructions and Combinatorial Problems in Design of Experiment, New York, 1971.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

只有在阶数 v 能被 4 整除时，反对称 C 矩阵才能够存在．只有在 $v-2$ 能被 4 整除且 $v-1$ 为两个整数的平方和时，对称的 C 矩阵才存在．但是，整数 n 为两数的平方和，当且仅当 n 的平方剩余没有模 4 余 3 的素因子．因而，不存在 22 阶的对称 C 矩阵．

我们已经碰到过 4，6，10 阶为 C 矩阵（彼德森图的邻接矩阵）．现在，我们通过例子给出 8 阶 C 矩阵的一个构造法．这个方法是佩利[①]给出的，可以推广到所有奇素数幂 $v-1$ 的情形．

模 7 的剩余类分别为 7 的倍数加上 0，1，2，3，4，5，6，我们把它们记为 $a_0, a_1, a_2, a_3, a_4, a_5, a_6$．显然，$a_1, a_2, a_4$ 是平方数，而 a_3, a_5, a_6 是非平方数．对任一类 $a_i - a_j (i, j = 0, 1, \cdots, 6)$，赋值为：

0，若 $a_i - a_j = a_0$；

+1，若 $a_i - a_j$ 是一个非零平方数；

−1，若 $a_i - a_j$ 是一个非平方数．

则这些“勒让德符号”（Legendre symbols）的矩阵是一个 7 阶的循环矩阵，其第一行为（0，−，−，+，−，+，+）．对这个矩阵镶边（增加第一行和第一列），便得到一个反对称的 C 矩阵：

$$C_8 = \begin{pmatrix} 0 & + & + & + & + & + & + & + \\ - & 0 & - & - & + & - & + & + \\ - & + & 0 & - & - & + & - & + \\ - & + & + & 0 & - & - & + & - \\ - & - & + & + & 0 & - & - & + \\ - & + & - & + & + & 0 & - & - \\ - & - & + & - & + & + & 0 & - \\ - & - & - & + & - & + & + & 0 \end{pmatrix}.$$ [309]

① 见第 112 页所引用的论文．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

射影平面　6 维单形的 7 个顶点用 7 维空间中的下述 7 个点来表示：

$$(1,0,0,0,0,0,0),(0,1,0,0,0,0,0),\cdots,(0,0,0,0,0,0,1).$$

则这个 6 维单形的 35 个三角形中心的坐标为：

$$\frac{1}{3}(t,1,1,0,0,0,0),\frac{1}{3}(1,1,0,1,0,0,0),\text{等等}.$$

现在我们考虑这样一个问题：能否从中选取 7 个中心再构成一个 6 维单形？这意味着每对所要求的中心都有一个公共坐标 1. 这便又回到第 277 页的出发点，事实上，射影平面 PG(2,2)的关联矩阵的 7 个行向量便提供了一个答案.

让我们简要地回顾一下本章所遇到的某些组合设计问题.

令 V 是包含 v 个元素的有限集合，k 和 λ 是满足 $0<k<v-1$，$0<\lambda$ 的整数. 一个（均衡而不完备的）区组设计 (v,k,λ) 是 V 的一组子集，其中每个子集包含 7 个元素（叫做 V 的 k 阶子集），并且 V 的每个 2 阶子集都含在这些 k 阶子集中的 λ 个中. v 阶施泰纳三元系便是这样的例子，其中 $k=3$，$\lambda=1$.

如果子集组中包含的 k 阶子集的数目等于 V 中元素的个数，则这一区间设计是*对称的*. 例如：任一规范化的 $4t(\geqslant 8)$阶阿达玛矩阵便等同于一个对称的区组设计，其参数为

$$v=4t-1,\quad k=2t-1,\quad \lambda=t-1.$$

n 阶的*有限射影平面*是参数为

$$v=n^2+n+1,\quad k=n+1,\quad \lambda=1$$

的一个对称的区组设计. V 中的元素是点，k 阶子集是平面中的直线. 由 $n-1$ 个两两正交的 n 阶拉丁方构成的完全组等于一个 n 阶的射影平面.

[310]　这并不意味着，给定任意的 v,k,λ，相应的区组设计都能够构造出来. 已经知道了某些不存在性的定理，同时某些区组设计也具体构造出来，但仍有很多是未知的. 有限射影平面只对阶数为素数幂的情况构造了出来；有时对同一个阶数存在几组不

我们必须知道，而且我们必将知道

http://maths352.bokee.com

同构的构造结果.我们还知道一个由布鲁克(R.H.Bruck)和赖瑟(H.J.Ryser)给出的不存在性定理①:如果 n 满足:$n \equiv 1$ 或 2 (mod4),$n \neq a^2 + b^2$,a,b 为整数,则不存在 n 阶的射影平面.这就排除了 $n = 6$ 的情况.第一个未明确的情况是 $n = 10$.欲知更详细的情况,请参阅文献②. [311]

① R.H.Bruck and H.J.Ryser, Canadian Journal of Mathematics, 1949, Vol. Ⅰ, pp. 88—93.

② P.Dembowski, Finite Geometries, Berlin, 1968; H.J.Ryser, Combinatorial Mathematics, Mathematical Association of America, 1963.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第11章 各种游戏

在本章中我要介绍几种常见的数学游戏的数学理论.本来可以在前四章中介绍它们,只因它们之中多半既涉及几何又涉及代数,所以把它们和前边讲过的问题分开来谈更方便些.至于本章内的安排只是以方便为原则而不是有什么逻辑关系.

这里列举的问题的大部分是彼此无关的,所以我差不多是随手写下去.

讨论的次序是"华容道"①、"河内塔"、"九连环"②,然后是几个关于纸牌的各种游戏问题.

华 容 道③④

数年前几乎所有的玩具店里都有这种玩具出售.它包括带

① 原文有人直译为"十五棋子戏",但这里讲的游戏可以不限于子数为15,也不一定用棋子.在我国有"华容道"棋和这里的游戏虽不尽同而极为相近,故采用其名.——译者注

② 我国的传统游戏,环数原则上也不限于9.——译者注

③ 关于这个游戏在 American Journal of Mathematics, 1879, Vol. II 上有 W·约翰逊(Woosley Johnson)教授和斯托里(Storey)教授的两篇文章.但全部理论皆可由下文中的定理导出.

④ 华容道(国外直称为十五子戏)就是指定要某个子走到与空格(出口)相邻的位置上.借三国人物故事而得此名.这个游戏又称为"船坞排挡",也很贴切.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

有号码 1,2,3,…,15 的 15 个小方块和一个正方形的木制浅盘，四周有凸缘.木盘刚能容纳 16 个小方块并稍能松动.实际只有 15 个小方块(棋子)，所以它们可以在盘子里相对滑动.开始时把 15 个子随便放入棋盘而让第 16 个格子空着.游戏要求滑动(不许拿起来)棋子使它们终于排列成指定的次序，例如下边的左图所示. [312]

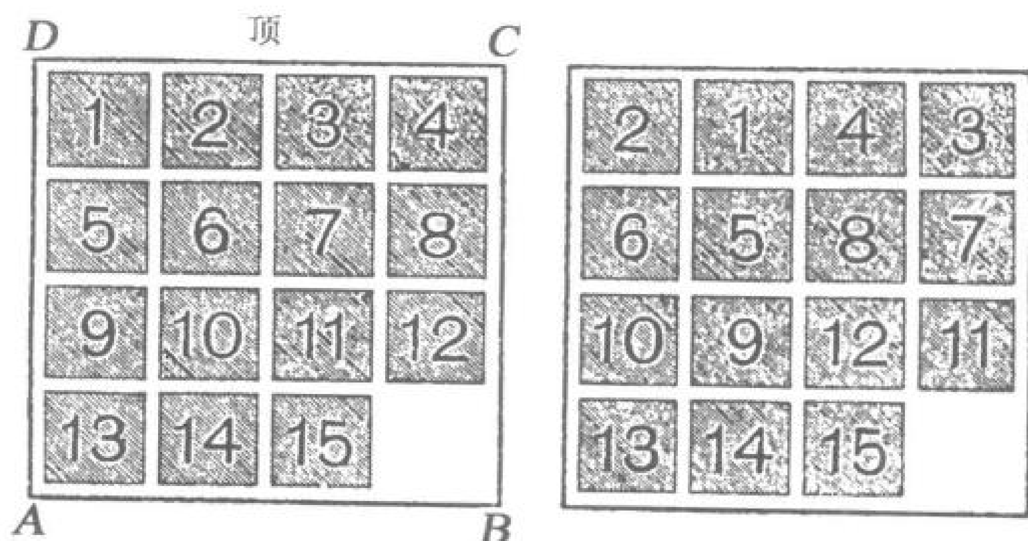


图 11.1

我们可以把游戏的各个进程看成是开始时处于第 16 号格子的空位置在游动，最后它仍回到出发时所在的地方.

空位置游动的路线可以包含两种阶段.一类是走几步又沿原路退回去，这对棋子的排列不产生影响，另一类是沿闭路线循行一周，这必然使奇数个棋子作循环置换——轮换.不会有别的情况了.

我们知道，n 个字母的循环置换等价于 $n-1$ 次简单的交换，即 $n-1$ 次的两两"对换".于是，奇数个字母的轮换等于偶数个对换之积.因此，如果棋子的走动使空位置游回原地，那么棋子的新次序与开始时的次序必然相差偶数个对换.所以，如果希望得到的次序可以从原次序经过奇数个对换而得之，那么这问题是不可解的；如果它可以经过偶数对换而得之，那么这问题

我们必须知道，而且我们必将知道

http://maths352.bokee.com



就是可解的①.

图 11.1 的右图中的次序可以由左图经过六个对换而得出.这些对换是:交换棋子 1 与 2,3 与 4,5 与 6,7 与 8,9 与 10,11 与 12.所以,适当走动棋子,这两种次序是可以相互转
[313] 变的.

但是,如果右图中最后三个棋子的次序是 13,15,14,那么要把右图转化成左图就需要七个对换.所以在这种情况下问题是不可解的.

寻求从一个排列导出另一个排列所需要的对换数目的最容易的方法是分解成一系列的轮换链.例如,给盘中的棋子任意指定一个次序,譬如说从左到右并一行一行往下排,并假定初始时的次序和最终的次序分别是

1, 13, 2, 3, 5, 7, 12, 8, 15, 6, 9, 4, 11, 10, 14;
11, 2, 3, 4, 5, 6, 7, 1, 9, 10, 13, 12, 8, 14, 15.

我们可以从前者经过 12 个对换而导出后者.为了作出这个论断的最简单的办法是把上列序列分解成如下的三个相互分离的轮换链:

1, 11, 8;	13, 2, 3, 4, 12, 7, 6, 10, 14, 15, 9;	5.
11, 8, 1;	2, 3, 4, 12, 7, 6, 10, 14, 15, 9, 13;	5.

如果在上一行的数字中把 1 换成 11,然后把 11 换成 8,再把 8 换成 1,我们就完成了 3 个数字的轮换,它等价于两个对换(即,交换 1 和 11,然后交换 1 和 8).因此,整个转化过程等价于一组 3 个数字的轮换、另一组 11 个数字的轮换,和另一组 1 个数字的轮换.所以它等价于(2 + 10 + 0)个对换.这是个偶数,因而可以经过滑动盘子里的棋子而把一个次序转变成另一个次序.

---

① 参看 Mathematical Gazette, 1940, Vol. XXIV, p. 119(Note 1454)所载 H.V.Mallison 的文.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

明显的是,如果初始的次序和要求的次序除了最后三个棋子外其他都相同,最后三个棋子的初始次序是 15,14,13.要把它们变成 13,14,15,只需一个对换,因而问题是不可解的.

再者,如果把棋盘转过一个直角,使 AD 边成为上边,则这个转动将等价于 13 个对换.这是因为,如果我们保持第 16 号方 [314]
格仍是空格,则这一转动将把次序

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15

转化成

13, 9, 5, 1, 14, 10, 6, 2, 15, 11, 7, 3, 12, 8, 4.

这等价于 13 个对换.所以它能改变一个排列使不可解的问题变成可解的,使可解的问题变成不可解的.

再有,即使初始的次序是不可解的,然而空位置不是留在最后一个方格上而是留在第一个方格上,那么仍可以把 15 个棋子按自然顺序排列.这是因为,如果用 b 记空格,则这一要求等价于将序列

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, b

转化为

b, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,

而这个转化实际上就是 16 件东西的轮换,因而等价于 15 个对换.所以它能将排列改变使不可解的问题变为可解的,将可解的变为不可解的.

上述原理显然也适用于包含 mn 个格子或位置的长方形棋盘和 $mn-1$ 个带编号的棋子.当然,m 可以等于 n.当 m 和 n 都是偶数时(还有某些其他情况,如 $m=3, n=5$),把棋盘转过一个直角等价于进行奇数次的对换,因而不可解的问题变为可解的,可解的变为不可解的.相仿地,若 m 和 n 不都是奇数,则当空位置是留在最后一个格子上而问题是不可解的时候,可以把空位置改留在第一格上而使问题变成可解的.

这个游戏可以用在棋盘上加一些固定的隔墙而变得更为困 [315]

我们必须知道，而且我们必将知道

http://maths352.bokee.com

难.皮特欣(Piet Hien)发明了一种类似的立体游戏,称为集装盒(Bloxbox)①.

河 内 塔

下一段,我来叙述一个巧妙的游戏,称为"河内塔".它是1883年由克劳斯(M.Claus)(据吕卡斯认为)发明的.

这个游戏使用三个立柱和八个木制圆盘或厚纸片,它们每个的中心都有一个小孔,因而可以穿到立柱上.这些圆盘的半径各不相同.游戏开始时八个圆盘都穿在同一个立柱上,最大的圆盘在最下边,愈往上边的圆盘愈小,最小的在最上边.这种装置就叫做一个"塔".游戏的要求是把这些盘子转移到另一个立柱上去②,在转移的过程中任一个盘子永不许放在比它小的盘子的上方,而且最后要把整个塔(即保持各个盘子原来的相对层次)都转移过去.

实现这个目标的步骤如次:(i)假设最初有 n 个盘子穿在立柱 A 上.第一步是把上边的 $n-1$ 个盘子从立柱 A 上转移到立柱 B 上,立柱 C 最后仍然空着.假定这需要 x 次的转移.(ii)其次,将最下层的盘子转移到立柱 C 上.(iii)然后,反转第一步的过程,逐渐把 B 上的 $n-1$ 个盘子转移到立柱 C 上,这又需要 x 次的转移.所以,如果要转移一个 $n-1$ 层的塔需要 x 次的单盘转移,则转移一个 n 层的塔需要 $2x+1$ 次的单盘转移.显然,两个盘子需要 3 次转移,即 2^2-1 次.所以 3 个盘子需要 $2(2^2-1)+1$次转移,即 2^3-1 次.依此类推,可知一个 n 层的塔需要2^n-1次的单盘转移.故八个盘子的游戏需要 255 次的单盘
[316] 转移.注意,每轮转移都需要把最小的盘子从一个立柱先转移到

① Scientific American, 1973, Vol. CCXXVII, no.2, p. 103.

② 每次只许动一个盘子,可以借助于第三个立柱作为中转站.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

另一个立柱上,立柱被轮流取用;还有,如果把盘子从小到大连续编号为 1,2,3,…,则所有的奇数号盘子按一个方向轮转,所有偶数号的盘子按另一个方向轮转.

显然,盘子可换成带编号 1,2,3,…n 的厚纸片;如果 n 不大于 10,改用扑克牌也是很方便的.

德帕尔维伊(De Parville)写过一篇关于这种玩具起源的趣文,值得转述[1].他说,在贝那拉斯的大庙里,大殿的圆穹标志着世界的中心.圆穹下放着个大铜盘,铜盘里固定着三个细似蜂腰的宝石针,每棵针三尺高.上帝创造世界的时候,在其中的一棵针上穿放了 64 只赤金盘,最大的盘子在最下边紧坐在铜盘上,往上去一个比一个小.这就是梵天塔.长老们日夜不停地把金盘从一个宝石针遵照不可违犯的一定的婆罗门法规转移到另一个宝石针上,该法规说,值班的祭司每次只能转移一只金盘,并且只能转移到下边没有较小的金盘的宝石针上.当那 64 只金盘从上帝所穿的宝石针上全部被转移到另一棵宝石针上时,河内塔、大庙以及婆罗门人将统统化为灰烬,同时一声霹雳,世界也化为乌有.

婆罗门人为转移梵天塔而必须进行单个金盘分别转移的次数是 $2^{64}-1$,即,18 446 744 073 709 551 615.这个数字之大
使得最后的霹雳声响时宇宙的年龄比现在要大一千倍. [317]

九 连 环[2]

更复杂一些的种游戏是九连环,在西方称为“中国环”(即,

① La Nature, Paris, 1884, part I, pp. 285—286.

② 这是 1550 年卡尔丹所述的,见于他的 De Subtilitate,第 XV 编,第 2 段,Sponius 版,卷Ⅲ,p. 587;沃利斯(J. Wallis)也曾转述,见于他的 Algebra,拉丁文版,1963, Opera, 卷 Ⅱ,第 CXI 章,pp. 472—478;在奥札南的 Récréations (1723 版,卷Ⅳ,p.439)上也曾提到.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

九连环)，英国的多数玩具店里都有出售，其构造如图 11.2 所示. 它由一些套在一双棒上的小环组成. 这些小环又被细丝穿连在一起①. 最外端(如 A 端)的环可以随意从双棒上脱下或套上，而任一其他的环仅当在它的 A 侧与它紧邻的环套在双棒上而它侧其余的环都不套在双棒上时才可能从双棒上脱下. 各个环的相对次序是无法改变的.

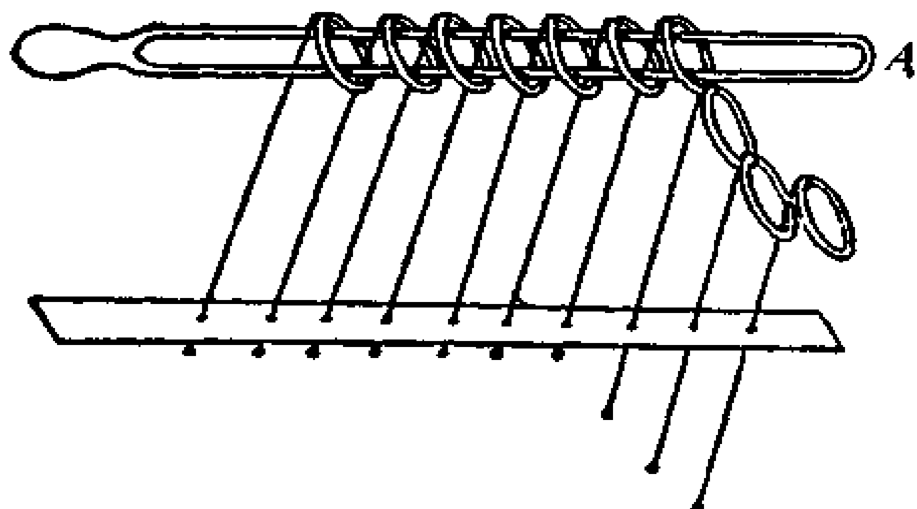


图 11.2

每次只可能脱下或套上一个环.(通常所出售的玩具的前两个环是例外，它们可以同时脱下或同时套上. 为了简化讨论，我将先假定每次只可脱下或套上一个环.)我来证明，如果有 n 个环，那么为了把它们统统脱下，当 n 为奇数时需要把单个的环脱下或套上$\frac{1}{3}(2^{n+1}-1)$次，当 n 为偶数时，需要$\frac{1}{3}(2^{n+1}-2)$次.

以下称将一个环从双棒上脱下或套到双棒上去为一“步”. 通常，环的编号从自由端 A 编起，称为第一环、第二环、……
[318] 再假定开始时前 m 个环已从双棒上脱下而其余的 $n-m$ 个环

① 一共几个环穿在一起就称为几连环. 通常用九个环，故称为“九连环”游戏. ——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

都在双棒上套着，并且为了把第 $m+1$ 个环从双棒上脱下需要 $x-1$ 步. 在进行这些步子之前，我们能够把第 $m+2$ 个环脱下，那么从我们的开始状态脱下第 $m+1$ 个环和第 $m+2$ 个环共需要 x 步.

假定这 x 步已实行过了，那么前 $m+2$ 个环已经从双棒上脱下，其余的环尚在双棒上套着. 我们来考查为了脱下第 $m+3$ 和第 $m+4$ 个环，需要再进行多少步. 为此，我们先脱下第 $m+4$ 个环，这只需 1 步. 在能够脱下第 $m+3$ 个环之前，必须做到第 $m+2$ 个环套在双棒上而前 $m+1$ 个环已经脱下. 为此，(i)必须把第 $m+1$ 个环套上去而把前 m 个环脱下来，这需要 $x-1$ 步；(ii)然后又需要把第 $m+2$ 个环套上去，这只须 1 步；(iii)最后还必须把第 $m+1$ 个环脱下来，这需要 $x-1$ 步. 这些动作共需 $\{2(x-1)+1\}$步. 然后，我们可以把第 $m+3$ 个环脱下来，这只需 1 步；其结果是前 $m+1$ 个环已脱下，第 $m+2$ 个环在双棒上，第 $m+3$ 和第 $m+4$ 个环被脱下，其余的环都还在棒上. 最后，要脱下第 $m+2$ 个环，须(i)把第 $m+1$ 个环套上去并且把前 m 个环脱下来，这需要 $x-1$ 步；(ii)脱下第 $m+2$ 个环，这只需 1 步；(iii)脱下第 $m+1$ 个环，这需要 $x-1$ 步. 这些动作共需 $\{2(x-1)+1\}$步.

所以，如果前 m 个环已不在棒上，要脱下第 $m+1$ 个和第 $m+2$ 个环，那么为脱下第 $m+3$ 个和第 $m+4$ 个环而需要的步数是 $1+\{2(x-1)+1\}+1+\{2(x-1)+1\}$，即 $4x$ 步.

为了求出脱下奇数个环所需的总步数，我们进行如下的分析：

脱下第 1 个环需要 1 步；

∴ 脱下前 3 个环又需要 4 步；

∴ 脱下前 5 个环又需要 4^2 步； [319]

……

依此类推，可知为了脱下前$2n+1$个环所需的总步数是$1+4+$

我们必须知道，而且我们必将知道

http://maths352.bokee.com

$4^2+\cdots+4^n$，即，$\frac{1}{3}(2^{2n+2}-1)$.

为了求出脱下偶数个环所需的总步数，可作相仿的分析.

脱下前两个环需要 2 步；

∴　脱下前 4 个环又需要 2×4 步；

∴　脱下前 6 个环又需要 2×4^2 步；

……

依此类推，可知为了脱下前 $2n$ 个环所需的总步数是 $2+(2\times 4)+(2\times 4^2)+\cdots+(2\times 4^{n-1})$，即 $2^{2n-1}-1$.

如果前两个环作为一步脱下而不分为两步，那么这两个结果分别是 2^{2n} 和 $2^{2n-1}-1$.

我给出上边的分析，因为它是 1550 年卡尔丹未能解决而 1693 年沃利斯也未能解决的问题的直接解答，这问题曾一度颇受注意.

以下我再给出另一个更漂亮的、而技巧性也更强的解答.这个解答是格罗斯(Gros)先生①给出的，它的关键是一个约定，根据这个约定，任一个环的任一位置可用二进位制数表示，而每一个步骤相当于在该数上加一或者减一.

假定用小圆圈表示一个环.如果环在棒上，就把小圆画在棒的上边；如果环已脱下，就把小圆画在棒的下边.图 11.3 表示的就是七连环的情况，其中前两个环不在棒上，以后的三个环在棒上，第六个环不在棒上，第七个环在棒上.

用数码 1 或 0 交替地表示从棒的左端起穿在棒上的那些环，并用与左方邻环②的数码相同的数码表示不在棒上的环，如
[320] 果最左端的环不在棒上，就用 0 表示它.

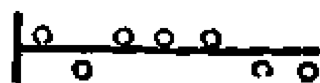
① Théorie du Baguenodier, by L. Gros, Lyons, 1872. 这里的阐述引自 Lucas, Vol. Ⅰ, part 7.

② 不论套在棒上或否，只论环的编号相邻.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

于是,下图所示的三种布局分别由它们下边的数码表示.将图 11.3 中第一个环套到棒上即得图 11.4,将图 11.3 中第四个环从棒上脱下即得图 11.5.



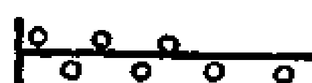
1101000

图 11.3



1101001

图 11.4



1100111

图 11.5

所以,环的每一种布局都由一个二进位数表示.此外,从左到右看时,与棒上的环对应的数码总是一个个交替地在变化(1 后边是 0,0 后边是 1)而与不在棒上的环对应的数码总是和它左边紧邻的数码相同,从棒上脱下一个环时相应的数字加 1,套上一个环时相应的数字减 1.例如,在表示图 11.3 的布局的数字上加 1 就得到表示图 11.4 的布局的数字,减 1 就得到图11.5 的布局的数字.

当所有的环都不在棒上时,相应的数字是 0000000,当所有的环都在棒上时,相应的数字是 1010101.所以由一个局势变成另一个局势时,需要的步数等于前后两个二进位数的差.这两个数中前一个是 0,后一个是 $2^6+2^4+2^2+1$,即 85,所以共需 85 步.相仿地,可以证明,要把 $2n+1$ 个环都套到棒上需要 $1+2^2+\cdots+2^{2n}$ 步,即$\frac{1}{3}(2^{2n+2}-1)$步,而要把 $2n$ 个环都套到棒上需要 $2+2^3+\cdots+2^{2n-1}$步,即$\frac{1}{3}(2^{2n+1}-2)$步.

下边给出一个图表,表明为了要脱下棒上的五连环的前四个环所需采取的步骤.下表中间一列的图表明了这些环在各个 [321]
步骤后的局势.每个图的右边的数字表明了相应的局势,在任一个数字上加一就得到下一个数字.花括号所括的两步可以一次完成,这样做时,整个过程就由 10 步减少为 7 步.这和上述公式是一致的.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

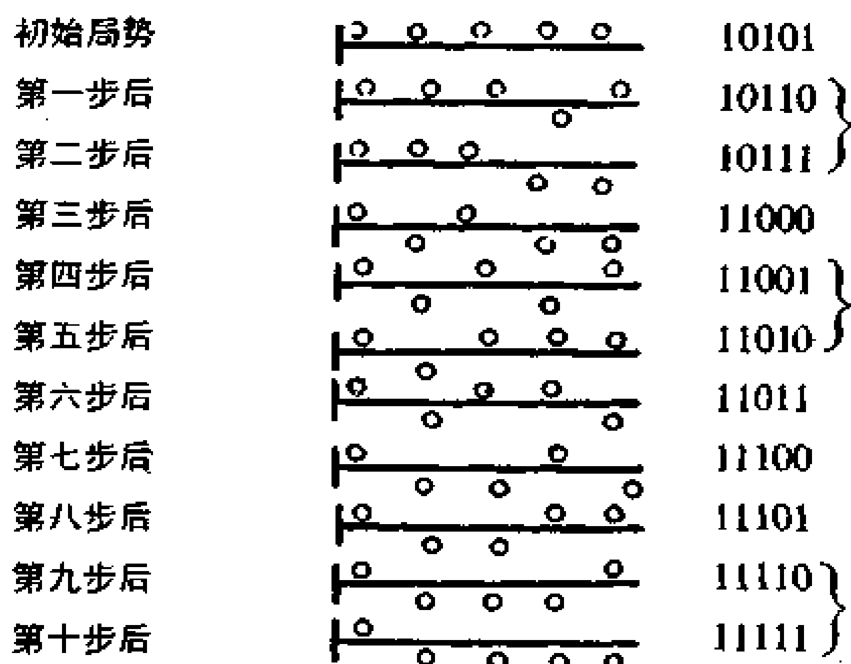


图 11.6

格罗斯认为一分钟可以进行 64 到 80 步，据我的经验，这是个偏高的估计. 如果我们接受这些步数的下限，那就是说：在不到 8 分钟里可以脱下一个 10 连环；要脱下一个 25 连环就需要 582 天以上，每天以 10 小时工作计算；要脱下一个 60 连环，将需进行的步数不少于 768 614 336 404 564 650，大约需要工作 55 000 000 000 年，当然，还要假定步步都不曾弄错.

纸 牌 游 戏

一副普通的纸牌（如扑克牌）可用以作多种关于牌面数字的
[322] 简单性质或各张牌的相对位置的游戏. 此类游戏的实质在于按某种特定的方式重新排列纸牌将某张牌转到某个一定的位置. 任何一种这类的重排方法谓之一种洗牌法.

我将依次论述以下几个游戏：洗牌，猜一张牌，（从$\frac{1}{2}n(n+1)$组牌里）猜一组牌；热尔岗（Gergonne）的摆物游戏，窗口里瞧，以及捉老鼠.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

洗　　牌

任何一种“洗牌”法，如果一直进行下去，都会达成一个可以算出来的排列；不过，靠洗牌来玩的游戏都需要熟练的技巧.

例如，一种洗法是(并非罕见)把一副 n 张牌的第 2 张放到第 1 张上边，第 3 张放到前两张的下边，第 4 张又放到前三张的上边，如此等等. 这种洗法的理论是蒙日(Monge)①建立的. 下边是一些结论，不难直接去证明.

一副 $2p$ 张的牌洗过一遍之后，原来的第 x_0 张变成第 x_1 张，当 x_0 为奇数时，$x_1=\frac{1}{2}(2p+x_0+1)$，当 x_0 为偶数时 $x_1=\frac{1}{2}(2p-x_0+2)$. 例如，全副 52 张扑克牌按上述洗法洗过一遍之后，第 18 张仍是第 18 张. 一副截取的 32 张扑克牌如上洗过一遍之后，第 7 张与第 20 张交换了位置.

再者，任何一副 n 张牌，如上洗过几遍之后(不超过 n 遍)，所有的牌都将恢复其原来的次序. 只要一旦原来最上边的一张 [323]
出现在最上边，全副牌的次序就都恢复了. 对于一副 $2p$ 张的牌，要求出次序恢复时洗的最少遍数，只须令 $x_m=x_0$ 而求出当 x_0 取值 1 到 $2p$ 时适合这个方程的最小 m 值.

---

① Monge 的研究载于 Mémoires de l'Académie des Science, Paris, 1773, pp. 390—412. 重新研究这个课题的人之中有 V. Bouniakowski, Bulletin physico - mathématique de St. Pétersbourg, 1857, Vol. XV, pp. 202—205, 在 Nouvelles Annales de Mathématiques, 1858, Bulletin, pp. 66—67 上有其综述；T. de St. Laurent, Mémoires de l'Académie de Gard, 1865; L. Tanner, Educational Times Reprints, 1880, Vol. XXXIII, pp. 73—75; M. J. Bourget, Liouville's Journal, 1882, pp. 413—434; H. F. Baker, Transactions of the British Association for 1910, pp. 526—528; P. H. Cowell, The Field, 2 April 1921, p. 444.

我们必须知道，而且我们必将知道

[redacted]

然而，如果将牌按原来的次序从下向上编号，则更容易得到此结果．这样做了之后，可以证明：如果洗过 s 次之后某一张牌处于从下往上数第 r 个位置，那么，原来从下往上数时的编号数是 $2^s\times r$ 与 $4p+1$ 的最接近的倍数之差．所以，如果为了恢复原先的顺序而需要洗 m 次，则 m 必为使 2^m+1 或 2^m-1 能被 $4p+1$ 整除的最小数字．不论一副牌共有 $2p+1$ 张或 $2p$ 张，这个数字都是一样的．如果玩的是一副截取的 32 张牌，那么洗 6 次就够了；如果牌的总数为 2^n 张，那么洗 $n+1$ 次就够了；如果玩的是全副共 52 张牌，那么洗 12 次就够了；对于一副 13 张牌来说，洗 10 次就够了；对于一副 50 张的牌来说，需要洗 50 次；等等．

一般地说，对于一副 n 张的牌，不论洗牌的规律如何，只要洗的次数充分多，整副牌最终都将恢复其原来的次序．确切地说，赫德森（W.H.H.Hudson）①曾证明：在洗牌次数未超过和数为 n 的所有数组的最小公倍数的最大者之前，这个现象必然要发生．

如果 $P_1,P_2,\cdots,P_n$ 代表各张牌可能处的位置，那么每次洗牌可用一些不相干的“局部洗”或“链”的积表示之：

$$S=(P_aP_b\cdots P_i)(P_j\cdots P_m)\cdots(P_u\cdots P_z),$$

这里表明 P_a 被移到 P_b，链中最后的一个位置（如 P_m）被移到该链中第一个位置（如 P_j）．由于这些局部洗是彼此无关的，它们

[324] 的次序的任何改变都不会影响整个的洗牌；因此，S 的两次实现可以写成

$$S^2=(P_aP_b\cdots P_i)^2(P_j\cdots P_m)^2\cdots(P_u\cdots P_z)^2.$$

可以验证，位置属于某个周期（或“长度”）为 r 的链的每张牌在洗过 r 次之后必然要回到其原来的位置．如果对于某一特定的

① Educational Times Reprints, London, 1865, Vol. Ⅱ, p. 105. 也可参看 E. Landau, Archiv der Mathematik, und Physik, 1903, series 3, Vol. Ⅴ, pp. 92—103; W. Feller, An Introduction to Probability Theory, New York, 1950, pp. 335—341.

http://maths352.bokee.com

洗法来说，m 是各个链长的最小公倍数，则按这种洗法洗过 m 次之后，所有的牌都将恢复其原来的位置．于是对于一副 n 张的牌来说就得到赫德森的结论．例如，当 $n=52$ 时，我们知道任何洗法的周期都不会超过 180 180.

猜单张牌

用洗牌来打掩护的一种常见的奥秘是这样一个明显的事实．如果把 n^2 张牌排列成 n 行而每行有 n 张的一个正方形，那么任何一张牌只要指出它所在的行和所在的列就知道它是哪一张了．

这些信息通常是这样使对方吐露出来的．先问他所选定的牌是在哪一行里，并且注意该行最左端的一张牌．然后从左下角开始把最左列的牌从下往上一张一张面向上摞起来，后拿的放在先拿的牌的上边，然后把左边第 2 列也照样摞起来，接着向右去把第 3 列、第 4 列、……、第 n 列都摞起来．再把从左到右第 2 摞放到第 1 摞上、第 3 摞放到第 2 摞上，……，第 n 摞放到第 $n-1$ 摞的上边．接着再把牌一张一张从左上角开始向右摆成行、每行 n 张，从上到下 n 行．再问对方所选定的牌在哪一行里．他所选的牌就在该行中，同时在先前所注意的那张牌所在的列中．

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

图 11.7

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

图 11.8

这个游戏还可再作改进——在第二次摆开之前让对方任意切牌几次，最后自己再切牌一次使原先最上边一行中的随便哪一张牌出现在最上边．例如，假定只玩 16 张牌．第一次排开的样

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[325] 子如图 11.7，第二次排列的样子如图 11.8. 假定对方第一次回答说他选定的牌在第 3 行里，那就是 9，10，11 或 12；那么只要他第二次再回答他选定的牌在第几行里，你立即就知道是哪一张了. 如果让他第二次摆开前任意切牌，那么你就要想法让最上边出现的一张牌成为 1，或 2，或 3，或 4，因为这样就能保持第二图中每一行的牌不变，至多不过是行的次序变了.

猜一组牌①

另一种常见的游戏是把 20 张牌编为 10 组，每组 2 张，乱扔在桌子上而请某人心目中选定其中的一组. 然后把牌收起来再按一定方式排 4 行每行 5 张. 只要他说出他选的一组牌在哪一行或两行里，我立刻就知道是哪两张.

这个游戏的理论根据是 4 种符号能够构成 10 个二次单项式. 所以 4 种符号的两两乘积可用以表示 10 件事物.

假定把两张为一组的 20 张牌乱放在桌上后有人想好其中的一组. 现在我把它们一组一组收起来. 先收的两张算第 1 组，次收的两张算第 2 组，等等，最后收的两张算第 10 组. 然后把它们照下图的顺序排成 4 行，每行 5 张.

1	2	3	5	7
4	9	10	11	13
6	12	15	16	17
8	14	18	19	20

[326] 图 11.9

① Bachet，问题 XVII，avertissement，pp. 146 起.

我们必须知道，而且我们必将知道

第一组(1与2)放在第1行.第二组(3与4)的一张放在第1行,另一张放在第2行.第三组(5与6)的一张放在第1行,另一张放在第3行.照此办理.第1行放满之后①,接下去相仿地补充第2行,第2行放满之后②,接下去相仿地补充第3行,等等.

询问他所选的一组牌是在哪一行或两行里.如果他说都在某一行,譬如第 m 行里.那么他所选的必是该行里的第 m 张和第 $m+1$ 张.它们占有该行的"导引"位置.如果他说所选的一组牌在不同的两行里,那么作如下的分析.设他说的是第 p 行和第 q 行且 $q>p$.那么他所说的第 q 行的那一张牌就是第 p 行的第一个导引位置下向右数起第 $q-p$ 张牌,另一张就是第 p 行内第二个导引位置右边的第 $q-p$ 张牌.

以上我说的这种形式的巴协规则可以应用于分成两两一组的 $n(n+1)$ 张牌的此类游戏,要把它们排成 n 行,每行 $n+1$ 张,排法仿上.因为有 $\frac{1}{2}n(n+1)$ 组,而用 n 个符号可以形成 $\frac{1}{2}n(n+1)$ 个二次单项式.巴协给出过20,30,40张牌的排列图,读者自己不难去构制它们;我以20张牌为例说明的步骤与规则同样适用于一般情况.

我见过有人不用数字而用一句话玩这种游戏.以10组为例,那么在一组一组收起来后,就可以按照 Matas dedit nomen Cocis 这句话的字母的次序把牌排成4行、每行5张.必须在想象中把这句话写在桌面上,每个字占一行.第1张牌放在字母 M 上.第2张牌(它和第一张是一组)放在这句话中的第二个 m 字母上,即第3行的第三个位置.第3张牌放在字母 a 上.第4 [327]
张牌(它和第3张是一组)放在第二个 a 上,即第1行的第四个

① 此时第二行已有一张牌.——译者注

② 此时第三行已有两张牌.——译者注

http://maths352.bokee.com

位置上.其次的两张放在两个 t 上,如此等等.询问某人他选定的一组两张出现在哪些行上.如果回答说在某两行上,那么他选的两张就在分占该两行的那同一个字母上.如果回答说在某一行上,那么他选的两张就在那一行里两个相同字母上.

道理是明显的.令 a 表示第一组的每张牌,相仿地,其他各对分别用 e,i,o,c,d,m,n,s 或 t 表示之.语句 Matas dedit nomen Cocis 包括四个字,每个字由五个字母组成;一共用了十个字母,每个字母重复一次.所以,如果说了两个行,它们将有一个共同的字母;如果只说一个行,它也有两个字母相同.

用别种张数的牌玩这样的游戏时,各需一个不同的语句.

四个字母的三次单项式共有 20 种,其中三因子相同的和三个因子全不相同的共有 8 种.这就有可能用 8 个三重组进行与上述游戏相仿的游戏——按语句 Lanata levete livini novoto 所示的次序去排列 24 张牌.

我相信这种排语句排牌的玩法是众所周知的,但究竟是谁发明的,我一点也不知道.

热尔岗摞物游戏

在讨论热尔岗(M.Gergonne)的定理之前,我先说明一下熟知的三摞物问题,它的理论包括在热尔岗的结论里.

三摞牌问题① 这游戏的通常玩法如下.取 27 张牌,把它们分成三摞,牌面向上.这里说的"分"牌的具体做法是:最上边
[328] 的一张要作为第一摞的最下一张,第二张作为第二摞的最下一张,第三张作为第三摞最下一张,第四张要放在第一张的上边,等等.此外,在这个游戏中始终假定手中的牌都是面向上的.这里的结果可经修改而包括任何其他分牌的方法.

① 巴协曾提到过这个问题,见他的 problem XVIII, p. 143,但他的分析是不充分的.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

请一位旁观者注意一张牌，并记住它．分完牌之后，问他注意的那张牌是在哪一摞里．把三摞牌都拿起来并把他说的那一摞夹在中间．①重新再和前边一样把所有的牌分成三摞，再问他所注意的那一张牌是在哪一摞里．再把三摞牌都拿起来，仍把现在他说的那一摞夹在中间．再和前边一样进行分牌，但在分时注意每一摞正中间的那一张．第三次再问他注意的那一张在哪一摞里，你就会知道他所注意的那一张牌就是那一摞里你已经注意过的正中间的那一张．游戏至此可以任何方式结束．通常的方式——但是一个非常拙笨的方式——是再一次把三摞牌都拿起来，把最后说的那一摞夹在中间，这时他所选中的牌就是整副牌正中间的那一张了，即，如果用的牌一共 27 张，那就是第 14 张．

这个游戏也常用 15 张或 21 张牌来玩，不管哪种情况，上述规律都适用．

热尔岗的推广　热尔岗②给出了一副 m^m 张牌的此种游戏的一般理论．假定把这样一副牌分成 m 摞，每摞 m^{m-1}张，并且在第一次分牌后，选中的牌所在的那一摞作为第 a 摞而收牌；第二次分牌后，选中的牌所在的那一摞作为第 b 摞而收牌；如此等等；最后第 m 次分牌后，选中的牌所在的那一摞作为第 k 摞．那么，第 m 次再收牌后，选中的牌将必是从顶上往下数的第 n 张牌，这里

当 m 为偶数时，　$n = km^{m-1} - jm^{m-2} + \cdots + bm - a + 1$，

当 m 为奇数时，　$n = km^{m-1} - jm^{m-2} + \cdots - bm + a$．

例如，如果玩 256 张牌（即 $m = 4$），旁观者认准其中一张．那么玩时可每次把牌分成四摞，每摞 64 张，问他认准的牌在哪 [329]

① Gergonne's Annales de Mathématiques, Nimes, 1813—1814, Vol. Ⅳ. pp. 276—283.

② 其他两摞哪一摞在最上，哪一摞在最下，没关系．第二次与第三次亦然．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

一摞里.再收再分,经过四次分牌而询问后,就可以知道他认准的是哪一张了.原因是,第一次分牌并询问后,你知道它必在哪一摞(64 张)里了.第二次分牌时,这 64 张被等分到四摞里,再一问就知道在哪一组 16 张里了.第三次分牌后再问后,你已知道它在哪一组 4 张里.第四次分牌后再一问,他的回答就等于告诉你是哪一张了.

此外,如果玩 256 张牌,那么在每次分牌后,各摞收起的次序无关紧要.因为如果第一次分牌后选中的牌所在那一摞作为第 a 摞而被拣起,第二次作为第 b 摞,第三次作为第 c 摞,第四次作为第 d 摞,则该牌就是整副牌摞在一起时从顶上往下数时的第 $64d-16c+4b-a+1$ 张牌,所以是知道的.其实,第四次分牌后无须再收起来,因为一样的论证可以得知它是最后指出的那一摞中第 $64-16c+4b-a+1$ 张牌.例如,若 $a=3,b=4,c=1,d=2$,则该牌即是第四次指出的那一摞中的第 62 张,如果都收起来,则为整副中的第 126 张.

完全相仿,可以玩 27 张牌,分牌三次,每次分成三摞,每摞 9 张,就可以问出选的是哪一张了.如果各次如上分牌后,指出包含所选的牌的那一摞被作为第 a,第 b,第 c 摞而收起,那么所选中的牌就是整副牌中的第 $9c-3b+a$ 张,或者第三次分牌后所指的那一摞中的第 $9-3b+a$ 张.

证明的方法只需以通常玩 27 张牌($m=3$,分成三摞、每摞 9 张)的情况为例就足以说明了.

假定第一次分牌后,包含选定的牌的那一摞被作为第 a 摞而收起,那么(i)在整副牌摞中该摞的上边有 $a-1$ 摞(每摞 9 张);(ii)接着是包含该牌那一摞 9 张;(iii)再往下去是整副中其余的牌.这时牌被第二次分摞,在新的每一摞的最下边有 $3(a-$
[330] $1)$张来自(i),接上去 3 张来自(ii),其余 $9-3a$ 张来自(iii).

假定第二次指出包含选定的牌的那一摞又作为第 b 摞而被收起.那么(i)在整副牌摞中该摞的上边有 $9(b-1)$张;(ii)

我们必须知道，而且我们必将知道

http://maths352.bokee.com

然后是 $9-3a$ 张；(iii)再往下三张里有一张是选定的牌；(iv)最下边是整副中其余的牌．这时进行第三次分牌．在每一摞的最下边有 $3(b-1)$ 张来自(i)，接上去 $3-a$ 张来自(ii)，再接上去的一张是(iii)中的 3 张之一，其余是来自(iv)的 $8-3b+a$ 张．

所以，这次分牌之后，一旦指出是哪一摞，立即就知道选定的牌是该摞中从上往下数第 $9-3b+a$ 张．如果继续把该摞作为第 c 摞而把整副牌收起，选定的牌在整副牌中就是从上边数起第 $9(c-1)+(8-3b+a)+1$ 即第 $9c-3b+a$ 张．

由于第三次分牌后，所选牌在指出的一摞中的位置已经很容易找到了，所以游戏已可径行结束而无须再次收起．

如果每次都把指出的一摞作为中间的一摞，则 $a=b=c=2$，因而 $n=9c-3b+a=14$，这就是前边所说的常见玩法．

上边已经证明：只要知道 a,b,c，那么 n 就被确定了．我们还可以修正法则使选定的牌出现在任何指定的位置上，譬如说，要它是整副牌摞中的第 n 张．这时，应求适合方程 $n=9c-3b+a$ 的 a,b,c 值，且 a,b,c 只能取值为 1，2 或 3．

于是，如果用 3 除 n 时余数是 1 或 2，则这个余数就是 a；但若余数是 0，那么就应将商减一而使余数为 3，这时 $a=3$．换句话说，a 是那样的最小非零正整数，当 n 减去它时，余数是 3 的整倍数．

其次，令此倍数为 p，即，p 为小于 $n/3$ 的最大正整数．于是
$3p=9c-3b$，所以 $p=3c-b$．因此 b 是那样的一个最小正整 [331]
数，当把它与 p 相加时，和数是 3 的一个整倍数，而这个倍数就是 c．

两个例子就会使以上所说更加清楚．假定我们希望选定的牌出现为从上往下数的第 22 张，那么 $22=9c-3b+a$．为了使差数是 3 的整倍数，应从 22 里减去的最小正整数是 1，故 $a=1$．于是 $22=9c-3b+1$，从而 $7=3c-b$．为了使和数是 3 的整倍

我们必须知道，而且我们必将知道

http://maths352.bokee.com

数，应加于7的最小正整数是2，故 $b=2$. 于是 $7=3c-2$，从而 $c=3$. 所以 $a=1,b=2,c=3$.

再一个例子. 假定我们希望选定的牌出现于第21个位置上. 那么 $21=9c-3b+a$. 为使差是3的整倍数，应从21里减去的最小正整数是3，故 $a=3$. 于是 $6=3c-b$. 所以 b 是当它加于6时和为3的整倍数的最小正整数，故 $b=3$. 于是 $9=3c$，从而 $c=3$. 所以 $a=b=c=3$.

如果说这样做还有什么麻烦的话，我们还可以改用如下的方式进行. 令 $a=x+1,b=3-y,c=z+1$；于是 x,y,z 仅能取值0，1或2. 这样一来，热尔岗的方程的形状化为 $9z+3y+x=n-1$. 于是，当 $n-1$ 换用三进位表示的时候，x,y,z 就被确定了，从而 a,b,c 也就找到了.

对于一副牌具有 m^n 张的情况，法则是一样的. 如果要选定的牌出现在指定的位置上，那么就要在热尔岗的公式里认为 n 是已知的而去求 $a,b,\cdots,k$. 为此可用 m 反复地去除 n，并约定要使余数呈正负交替地出现，并且它们的绝对值不大于 m 也不小于1.

对于一副牌具有 lm 张的情况也可以证明一个相仿的定理. 赫德森(C.T.Hudson)和迪克森①讨论过这种一般情况，要分牌 n 次，每次分成 l 摞，每摞 m 张；他们还曾阐明如何把各摞收
[332] 到一起，使得分牌 n 次之后选中的牌恰好是从上向下数第 r 张.

原理可以用一个与前边相仿的例子予以说明. 例如，假定把一副截取的32张牌分为四摞，每摞8张，在收牌时，包含选定牌的那一摞作为第 a 摞而收起. 再假定下一次分牌时，又指出某一摞包括着选定的牌. 这选定的牌不可能在最下边的 $2(a-1)$

---

① Educational Times Reprints, 1868, Vol. IX, pp. 89—91; Bulletin of the American Mathematical Society, New York, April 1895, Vol. I, pp. 184—186.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

张里,也不可能在最上边的 $8-2a$ 张里,而必定在中间的两张里.游戏至此可以任何方式结束,例如用通常的模棱法,即,要某人从中选出一张,但他弄不清选的那一张是要弃掉的呢还是要保留的.

古尔马泰(M.R.Goormaghtigh)①已经确定了 l 与 m 必须满足的条件,保证在分牌三次(每次分成 l 摞、每摞 m 张,包含选定的牌的那一摞每次都作为第二摞而被收起)后,能够找出选定的牌在哪里.这条件是 $[(m+h)/l]=[(m+k)/l]$ ($=p$,譬如说),其中 $h=[m/l]$, $k=[(2m-1)/l]$.第三次分牌后,选定的牌是指出的那一摞里的第 $p+1$ 张.用通常的一副 52 张牌玩时,可以取 $l=4$, $m=13$;于是 $h=3$, $k=6$, $p=4$.三次分牌后,选定的牌就是指出的那一摞里的第 5 张.

窗 口 里 瞧

数年前有人利用一种带数字的穿孔卡经营游戏活动.这种卡片以 8 张为一组.经营者能够说出游戏者所选定的数字.这 8 张卡片中前 7 张上都开有一个窗子形状的小口,后 7 张的每一张上都有一些小于 100 的数字,顶上写着"是"字,最后 3 张的背面上也有些数码,第一张顶上写着一个"上"字.把每一张颠倒过来看时,顶上都写着一个"否"字.

这些卡片就是被用来确定某游戏者 A 君所选定的小于 100 的任何数字的.不妨称经营者为 B 君.B 首先将带数字 1 的卡 [333]
片放到桌上且使"上"字那一边在上方.B 然后取第二张卡片并问 A 他选定的数字在不在其上.如果 A 回答说是,则 B 就把第 2 张卡片放到第 1 张上并使"是"在上边;如果 A 回答说否,则 B 就把第 2 张牌颠倒置放使"否"在上方.然后 B 再问选定的数在不在第 3 张卡片上,并把它放到第 2 张卡片上,方向仍如上确

① Sphinx, 1936, pp. 113—115.

我们必须知道，而且我们必将知道

定.对于其余的第 4 至第 8 张卡片也如法处理.最后,把整个一摞 8 张翻过来,B 就从窗子里看到了 A 选定的数.

这个游戏已是广为流传的.在意大利、德国和伦敦都有出售.所用的方法是很明显的,我把这种卡片的做法留给有兴趣的读者去自己想一想.

显然,任何不超过 128 的数只需 7 张卡片就能够确定出来,它们每一张上有 64 个数.因为第 1 张卡片把全部数字分成两组,每组 64 个数,可以选取第 2 张卡片上的数字使每一组被分成两组,每组 32 个数,第 3 张卡片又把每个组分成 16 个数,如此等等.写在卡片上的数字和卡片上窗口开的位置都必须使适当地安排卡片的次序后,将卡片一齐翻过来则从前六张卡片的窗口里能够看到第 7 张卡片背面上露出来的那个选定的数字.数字的安排没有什么困难,但开窗口的几何问题就不那么容易了.下边我给出一个解决的办法.

如果用 7 张卡片做游戏,卡片的一种制作方法如下.在第 1 张卡片的"是"字的下边写上由 1 到 32 和由 65 到 96 这 64 个数;在第 2 张卡片上写 1 到 16,33 到 48,65 到 80,97 到 112;在第 3 张卡上写从 1,2,5,6 开始的四个等差级数,每个 16 项,公差皆为 8;在第 4 张卡片上写从 1,2,3,4,5,6,7,8 开始的八个等差级数,每个 8 项,以 16 为公差;在第 5 张卡片上写由 1 至 127
[334] 的奇数;在第 6 张卡片上写从 1,2,3,4 开始的四个等差级数,每个 16 项,以 8 为公差;在第 7 张卡片上写从 1 到 64 的所有正整数;在这张卡片上的"否"字必须写在卡片的左边沿上而不是写在它的下边沿上.在最后这一张卡片的背面按自然顺序写上从 1 到 128,其中 1 到 32 占第一象限,33 到 64 占第四象限,65 到 96 占第二象限但要转一个直角,97 到 128 占第三象限,也转一个直角.数字之间的空隙需要精心,但只要掌握了制作的原则并采用方格纸,这是不会有困难的.

窗口的开法如下:假定采用方格纸并把卡片分成四个大小

http://maths352.bokee.com

相等的象限,各带空白边.在第1张卡片上,将第二象限全部切掉作为窗口.在第2张卡片上,切掉第二象限的上半部和第三象限的上半部,共开两个窗口.在第3张卡片上,切掉第二象限的右半部和第三象限的右半部,也是两个窗口.在第4张卡片上,将第一象限和第三象限各分成四个等宽的水平长条,各切掉其第一条和第三条.在第5张卡片上,将第二象限和第三象限分成四个等宽的竖直长条,各切掉其第二条和第四条.在第6张卡片上,将第二象限和第三象限各分成八个等宽的水平长条,各切掉其第一、第三、第五和第七条.

注意,任一卡片的第一象限和第四象限上都不曾开窗口;所以每张卡片的正面都有地方写上64个数.这里说的制作方法是我的朋友科尔(R.A.L.Cole)设计的.

如果略去所有大于100的数,这个游戏可能更妙一些,因为128这个数明显地暗示着制作的方法.这样的话,我想采用7张卡片要比我在商店里看到的更胜一筹. [335]

捉老鼠,十三点

在本章的结尾,我来简述一下另一种纸牌游戏,叫做"捉老鼠".详细的讨论还颇有些麻烦.

玩法是这样的:将一组标着数码1,2,3,…,n的一组纸牌乱洗一通之后,牌面向上摆成一个圆圈.游戏人从任一张开始顺着一个绕向转圈同时点数.如果口中数到k时,点到的牌上的数码恰好也碰到k——这就叫做"捉住了"——这时游戏人就把这张牌取走,然后开始往下重新再数.按凯莱的规定,如果游戏人终于把所有的牌都取走了,那么就算他赢了,如果在任何时候他口里已经数到n而一只老鼠也未捉到,那么就算他输了.

例如,假定只玩4张牌,摆开后的相对次序是3214,游戏人从第1张牌点起,那么他将首先取走"2"号牌,接着第二次取走"1"号牌,但是再往下数时,他再也捉不住任何老鼠了.假定开始

我们必须知道，而且我们必将知道

http://maths352.bokee.com

时牌的相对次序是1423，那么只要他先从“1”号牌点起，他就会相继取走1,2,3,4号牌.

问题的提法可以是：给定牌的数目之后，能捉住哪些老鼠和捉住几只老鼠，以及什么样的排列能按一定次序捉住一定数目的老鼠.

凯莱[①]曾证明：一副牌4张有9种排列能使你一只老鼠也捉不住，有6种排列能使你只能捉住一只老鼠，有3种排列能使你只能捉住两只老鼠，有6种排列可以把4只老鼠都捉住.

斯蒂恩(Steen)教授[②]曾研究过用 n 张牌玩捉老鼠的一般理论.他曾阐明怎样确定那种排列的数目，要“1”号牌首先被捉
[336] 住而且第二次捉住的一定是“x”号牌〔Art. 6〕；还有另一种排列的数目，要“2”号牌首先被捉住而且第二次捉住的一定是第“x”号牌；理论的进展未曾越过这一点.显然，如果捉住了 $n-1$ 只，那么第 n 只自然是跑不了的.

法国的“十三点”游戏和上述游戏非常相仿.这种游戏用的是一副52张扑克牌(J、Q、K分别当作11点、12点、13点).游戏人在每次开始前先讲好赢时赢多少、输时输多少.然后在顺次取13张牌的同时呼叫1,2,3,…,13.以叫号碰上所取牌的点数为
[337] 赢，否则为输(参看第47页).

① Quaterly Journal of Mathematics, 1878, Vol. XV. pp.8—10.

② 前注，Vol. XV, pp. 230—241.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第 12 章 三个古典的几何问题

古代的几何问题中更有趣的是早期希腊数学家特别感兴趣的三个问题.我们的几何学知识是从希腊发源的,因而这三个问题在几何学中有着很高的地位.我说的三个问题是:(i)二倍立方体——求一立方体的棱长,要它的体积是已知立方体体积的两倍;(ii)三等分角;(iii)化圆为方——求一正方形的边长,要它的面积等于已知圆的面积.每个问题都限于用直线和圆去构图解决,即据欧几里得几何学去解决.

限用直线和圆,这意味着在欧几里得几何学里许可使用的仪器只有直尺和圆规.当然,圆规的两脚必须要开多宽就能开多宽、直尺要多长就有多长.此外,直尺上不许有刻度,因为如果尺上有两个固定的记号,我们将能得到和利用圆锥截线所作等价的图形.

在上述欧几里得限制条件之下,所有三个问题都是不可能解决的①.为了二倍一个棱长为 a 的立方体,需要求作出一个长度为 x 的线段,它应适合 $x^3 = 2a^3$.为了三等分一个给定的角,可以先求出这个角的正弦 a,如果所给角的三分之一的正弦是 [338]

---

① 参看 F. C. Klein, Vorträge über ausgewählte Fragen der Elementargeometrie, Leipzig, 1895; F. G. Texeira, Sur les Problèmes célébres de la Geométrie Élémentare non resolubles avec la Règle et le Compas, Coimbra, 1915.据说,这些问题据欧几里得几何作图求解的不可能性的最早的严格证明是旺采尔(P. L. Wantzel)于 1837 年给出的.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

x，那么 $4x^3=3x-a$. 可见，从解析的方面看，第一个问题和第二个问题都需要解一个三次方程. 再者，用圆（其方程的形状是 $x^2+y^2+ax+by+c=0$）和直线（其方程的形状是 $\alpha x+\beta y+\gamma z=0$）构成的图线不可能和一个三次方程的解等价，因而可知如果限于用圆规和直尺作图，上边两个问题都是不可解的. 如果允许用圆锥截线，那么，这两个问题都可以按许多不同方法解决. 第三个的性质有所不同，但在同样的限制下也是不可解的.

以下我给出为解决前两个问题而提出的作图法. 为节省篇幅，将不画所需的图形，且在大多数情况下将也不加证明；后者略有困难. 最后以化圆为方的近似解法的几点历史注记来结束本章.

二倍立方体①

古时候把二倍立方体问题叫做德利安（Delian）问题，据稗史载，德利安曾就这个问题请教过柏拉图（Plato）. 在菲洛波纳斯（Philoponous）②所述的一个故事里说：公元前 430 年雅典人里伤寒病突然流行，他们去德洛斯（Delos）询求神谕怎样制止病疫. 太阳神阿波罗（Apollo）降谕，他们必须把他的祭坛的大小增加一倍，其形状为正立方体. 对于那些无知识的哀恳者来说，这似乎是再容易不过的了，他们马上建造了一个新的祭坛，其棱长为旧祭坛棱长的两倍（其体积为原来的八倍），又把一个完全相仿的正立方祭坛与原来的并排靠
[339] 放在一起. 为此，稗史称，大神变本加厉，瘟疫益发蔓延，并显示给一新的先知：亵渎大神是有罪过的，新的祭坛必须是体积为旧祭坛体积二倍的正立方体. 雅典人觉得内有奥秘，就去请教于柏拉图，柏拉

① 参看 Historia Problematis de Cubi Duplicatione by N. T. Reimer, Göttingen, 1798; Historia Problematis Cubi Duplicandi by C. H. Biering, Copenhagen, 1844；以及 Das Delische Problem, by A. Sturm, Linz, 1895—1897. 在我编的 History of Mathematics 里有关于这个课题的一些注记.

② Philoponus ad Aristotelis Analytica Posteriora，卷 I，第 2 章.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

图让他们去找几何学家们.故事里拉进去了柏拉图显然有年代上的错误.厄拉托斯特尼(Eratosthenes)①讲过一个相仿的故事,但是说这问题是米诺斯(Minos)提出的.

在一部阿拉伯著作里,希腊稗史又被讹误成如下的一段荒唐史,我把它引为一则奇文.作者说:"柏拉图在世的时候,以色列儿童中暴发一场瘟疫.于是上天向一位先知传来了声音,说'立方祭坛加一倍,瘟疫鬼头即粉碎';于是众人另做了一个和原来同样的祭坛,把它和旧祭坛并放在一起.然而疫情蔓延日甚一日.这时神声又向先知说:'两个祭坛排成队,岂乃立方体加倍?体积虽倍形长方,亵渎我神尔等罪!'于是众人向希腊哲人柏拉图请教.哲人告以'几何学为众科学中至为崇美卓绝之学科,尔等竟无视之,神灵以故乃施惩罚.'至于二倍立方体,它取决于几何学中一少见的问题,即,……"往后是阿波罗尼奥斯(Appolonius)的解,其法后详.

设所给立方体的棱长为 a,所求立方体的棱长为 x,$x^3=2a^3$,即,$x:a=\sqrt[3]{2}:1$.可能希腊人已意识到这个比值是无理的,即,任何两个整数的比皆不等于$\sqrt[3]{2}:1$,但不能从此得出结论说不能用几何方法找到这个比.事实上,一个正方形的边长和对角线长就是不可公度的线段的例子.

以下我来给出几个为解决二倍立方体问题而设计的几何作 [340]
图②.除了其中一个之外,我限于介绍借助于圆锥截线的作图.

希波克拉蒂斯解法 在解决这个问题上作出迈步的最早的

① Archimedis Opera cum Eutocii Commentariis, ed. Torelli, Oxford, 1792, p.144; ed. Heiberg, Leipzig, 1880—1881, Vol. Ⅲ. pp.104—107.

② 关于传统的希腊分析法在此问题上的应用可参看 Geometrical Analysis by J. Leslie, Edinburgh,第2版,1811,pp.247—250、453,其中包括希罗(Hero)与菲洛(Philo)法(导致用阿波罗尼奥斯(Apollonius)圆的解法)、尼科米迪斯(Nicomedes)法(导致利用蚌线的解法)、帕普斯法(导致利用蔓叶线的解法).

我们必须知道，而且我们必将知道

http://maths352.bokee.com

数学家大概是公元前大约 420 年的希波克拉蒂斯(Hippocrates)①.他没有给出几何作图解法,但是他把问题化归于求两个线段的两个平均值,一个线段的长度为(a),另一个线段的长度为($2a$).假定这些平均值是 x 和 y,则 $a:x=x:y=y:2a$.由此推出 $x^3=2a^3$.现在,这问题总是以这个形式呈现的.以前把通过求这些平均值而解此问题的任一过程都叫做一个"连比中量法"(mesolabum).

阿尔希塔斯解法 这个问题的早期解法之一是阿尔希塔斯(Archytas)②于公元前 400 年左右给出的.他的作图与下述作图是等价的.在一个正圆柱体的底的直径 OA 上立一个半圆,半圆所在的平面垂直于圆柱的底.令包含这个半圆的平面绕着过 O 的母线旋转,则半圆生成的曲面与圆柱面交出一条扭曲的曲线.此曲线和一个以 OA 为轴线而半顶角为 60°的正圆锥曲面相交于一点 P. OP 在圆柱底面上的投影与圆柱的半径之比就等于所求立方体棱长与已知立方体棱长之比.当然,阿尔希塔斯所给的证明是几何证明.有趣的是,证明中表明他对欧几里得原本卷Ⅲ.18;Ⅲ.35;与Ⅺ.19 中命题的结论都很熟悉.若要对他的作图的正确性作出解析的证明,可取 OA 为 x 轴,圆柱的过 O 的母线为 z 轴;然后采用通常的极坐标,令 a 表示圆柱的半径,则
[341] 半圆旋转所生曲面的方程是 $r=2a\sin\theta$;圆柱面的方程是 $r\sin\theta=2a\cos\phi$;圆锥的方程是 $\sin\theta\cos\phi=\frac{1}{2}$.这三个曲面交于一点,其坐标满足 $\sin^3\theta=\frac{1}{2}$,因此 $(r\sin\theta)^3=2a^3$.所以棱长为 $r\sin\theta$ 的立方体的体积是棱长为 a 的立方体的体积的两倍.

柏拉图作图法 公认为属于柏拉图③(公元前 360 年左右)

① Proclus, ed. Friedlein, pp.212—213.

② Archimedis Opera, ed. Torelli, p.143; ed. Heiberg, Vol.Ⅲ, pp.98—103.

③ Archimedis Opera, ed. Torelli, p.135; ed. Heiberg, Vol.Ⅲ, pp.66—71.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的作图法的依据是这么一个定理：若 CAB 与 DAB 为两个直角，AB 是它们的公共边，它们的另外两个边平行，斜边 AC 与 BD 垂直，相交于 P，则 $PC:PB=PB:PA=PA:PD$．于是，如果能作出一个这样的图，其中的 $PD=2PC$，则问题即可解决．不难制作一种仪器用以画这种图形．

梅内克缪斯解法 名字和二倍立方体联系着的下一个作者是梅内克缪斯(Menaechmus)[1]，他在大约公元前 340 年给出过两个解法．

在他的第一个解法里，他指出，两个具有共同顶点且其对称轴相垂直的抛物线，如果一个的通径是另一个的通径的二倍，则此两抛物线的另一交点的横坐标(或纵坐标)将给出问题的一个解．如果用分析的方法，这是很明显的．如果这两个抛物线的方程是 $y^2=2ax$ 和 $x^2=ay$，那么它们的交点的横坐标(除原点外)适合方程 $x^3=2a^3$．这个方法可能是受到了希波克拉蒂斯处理此问题的形式的影响，即，求适合于 $a:x=x:y=y:2a$ 的 x 和 y．显然这个条件可以化为 $x^2=ay$ 及 $y^2=2ax$．

梅内克缪斯的第二个解法如下：作一通径为 l 的抛物线．然后再画一条实轴长为 $4l$ 且以抛物线顶点处的切线和对称轴为渐近线的正双曲线．于是这两条曲线的交点的纵坐标与横坐标就是 l 与 $2l$ 之间的连比中项．两个曲线的方程是 $x^2=ly$ 和 $xy=2l^2$．它们的交点决定于方程 $x^3=2l^3$ 和 $y^3=4l^3$．所以 [342]

$$l:x=x:y=y:2l.$$

阿波罗尼奥斯作图法 阿波罗尼奥斯(Apollonius)的解[2]大

---

① Archimedis Opera, ed. Torelli, pp. 141—143; ed. Heiberg, Vol. Ⅲ, pp. 92—99.

② Archimedis Opera, ed. Torelli, p. 137; ed. Heiberg, Vol. Ⅲ, pp. 76—79. 这个解法载于我的 History of Mathematics, London, 1901, p. 84.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

约提出于公元前220年，具体如下：问题是要求两已知线段间的两个比例中项．以已知线段 OA 与 OB 为两邻边作一长方形 $OADB$．取 AB 的中点 C 为圆心作那样一个圆，它交 OA 的延长线于 a，交 OB 的延长线于 b 并使 aDb 成一直线．如果作出了这个圆，那么 $OA:Bb=Bb:Aa=Aa:OB$，即 Bb 与 Aa 就是 OA 与 OB 之间的两个连比中项．依欧几里得几何学的方法是作不出这样的圆的，但是阿波罗尼奥斯给出了画这个圆的机械方法．

狄俄克利斯作图法　我要介绍的仅有的另一个古代作图法是狄俄克利斯（Diocles）和斯波拉斯（Sporus）的作图法①，其法如次：以已知线段 OA 与 OB 为两邻边作长方形．假定 OA 大于 OB．以 O 为圆心，OA 为半径作圆．延长 OB，与圆交于 C；延长 AO 与圆交于 D．在 BC 上找一个那样的点 E，要 DE 与 AB 的延长线的交点 F 和它与圆的交点 G 合于 $FE=EG$．如果能够找到这样的一个点 E，那么 OE 就是 OA 与 OB 之间的第一个连比中项．狄俄克利斯为了确定点 E 而发明了蔓叶线，不过，借助于圆锥截线同样也能很方便地找到这个点．

近代又提出了一些别的解法．我顺便指出惠更斯（Huygens）②提出过三个解法，不过，我将只说明韦达（Vièta）、笛卡儿（R.Descartes）、圣樊尚（St. Vincent）的格雷戈里（Gregory）、以及牛顿（I.Newton）的那些方法．

韦达作图法　韦达的作图法是这样的③：以 O 为圆心并以两已知线段中较长者之半为半径作圆．在此圆内作一长度等于
[343] 两线段中较短者的弦 AB．将 AB 延长到 E，使 $BE=AB$．过 A 作 AF，平行于 OE．过 O 作直线 $DOCFG$，与圆交于 D 和 C 并与 AF

① Archimedis Opera, ed. Torelli, pp. 138, 139, 141; ed. Heiberg, Vol. Ⅲ, pp.78—84, 90—93.

② Opera. Varia, Leyden, 1724, pp.393—396.

③ Opera Mathematica, ed. Schooten, Leyden, 1646, prop. V, pp.242—243.

我们必须知道，而且我们必将知道

[redacted]

交于 F,交 BA 的延长线于 G,使 $GF=OA$.如果能够作出这条线,那么,线段 GC 与 CA 就适合

$$AB:GC=GC:GA=GA:CD.$$

笛卡儿作图法 笛卡儿曾指出①,曲线

$$x^2=ay \quad 与 \quad x^2+y^2=ay+bx$$

的交点 (x,y) 的坐标适合 $a:x=x:y=y:b$.当然,这和梅内克缪斯的第一解法是等价的,不过笛卡儿宁可用一个圆而不用第二条抛物线.

格雷戈里作图法 此法以下列定理②的形式给出.过矩形两边的交点而以其余两边为渐近线的双曲线和此矩形外接圆的交点到渐近线的两个距离是矩形两邻边的两个连比中项.这是曲线 $xy=ab$ 与 $x^2+y^2=ay+bx$ 交点 (x,y) 的坐标适合 $a:x=x:y=y:b$ 这一命题的几何表述.

牛顿作图法 牛顿的作图法之一如下③:令 OA 为两已知线段中的较长者.B 为 OA 的中点.以 O 为中心,OB 为半径作圆.在圆周上取一个点 C,使 BC 的长与两已知线段中的较短者.自 O 作 ODE,它与 AC 的延长线交于 D,与 BC 的延长线于 E,要使 $DE=OB$.于是 $BC:OD=OD:CE=CE:OA$.所以 OD 与 CE 是任意两线段 BC 与 OA 之间的两个连比中项.

三 等 分 角④

三个古典问题的第二个是三等分角,但传统上没有把它的

---

① Geometria,卷Ⅲ, Schooten 版,Amsterdam, 1659, p.91.

② Gregory of St. Vincent, Opus Geometricum Quadraturae Circuli, Antwerp, 1647,卷 Ⅵ,命题 138,p.602.

③ Arithmetica Universalis, Ralphson's 第2版, 1728, p. 242; 又 pp. 243,245.

④ 关于这个问题的文献可参看 L' Intermédiaire des Mathématicians 的补篇,Paris, May and June 1904.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[344] 来源纳入稗史.下述两个作图法是最古老的,也是最为人熟知的.帕普斯引述过它们①,但我不知道究竟是何人最先提出的.

帕普斯作图法 第一个作图法如下:设 AOB 为已知角.从 OB 上的任一点 P 作 PM 垂直于 OA.过 P 作 PR 平行于 OA.在 MP 上取一点 Q,OQ 的延长线交 PR 于 R,使 $QR=2\cdot OP$.如果能够作出这个构图,那么 $AOR=\frac{1}{3}AOB$.这个解法的关键是定出 R 的位置.从解析的角度看,这个要求可以如下实现.设已知角为 $\tan^{-1}(b/a)$.作双曲线 $xy=ab$ 和圆 $(x-a)^2+(y-b)^2=4(a^2+b^2)$.令 x 表它们的交点的横坐标中最大者,那么 $PR=x-a$ 而 $\tan^{-1}(b/x)=\frac{1}{3}\tan^{-1}(b/a)$.

第二个作图法如下:设 AOB 为已知角.取 $OB=OA$,以 O 为中心,OA 为半径作圆,充分延长 AO 到圆外,在此圆外的延线上取一个那样的点 C,若 CB 与圆的交点为 D,则 $CD=OA$.作 OE 平行于 CDB.若作出此图,则 $AOE=\frac{1}{3}AOB$.古人利用蚌线确定点 C 的位置,但也可以利用圆锥截线找到它.

我来给出几个其他解法,限于利用圆锥截线.

在帕普斯所给的其他诸法中,我转引下边的一个②.作一离心率为 2 的双曲线.设其中心为 C,两个顶点为 A 与 A'.将 CA' 延长到 S,使 $A'S=CA'$.以 AS 为弦作一圆弧使所含的角为已知
[345] 角.设 AS 的中垂线与此圆弧交于点 O.以 O 为中心,OA 或 OS 为半径作圆.此圆与双曲弧的过 A' 的那一枝的交点为 P.则

① Pappus, Mathematicae Collectiones, 卷Ⅳ, 命题 32, 33(Commandino 版, Bohn, 1670, pp.97—99).关于传统的希腊分析法在这个问题上的应用可参看莱斯利(J. Leslie)著 Geometrical Analysis, Edinburgh, 1811 年,第 2 版, pp.245—247.

② Pappus, Mathematicae Collectiones, 卷Ⅳ, 命题 34, pp.99—104.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

$SOP=\frac{1}{3}SOA$.

笛卡儿作图法 近代,直接用圆锥截线求解的最早解法之一是笛卡儿提出的,他用的是一个圆和一个抛物线.他的作图法①等价于求抛物线 $y^2=\frac{1}{4}x$ 和圆

$$x^2+y^2-\frac{13}{4}x+4ay=0$$

的除原点之外的交点.这些点的纵坐标适合方程 $4y^3=3y-a$. a 是已知角的正弦,较小的正根就是已知角的三分之一的正弦.证明是巧妙的.

牛顿解法 牛顿提出的解法之一实际和上述帕普斯的第三个解法是等价的.此法如下②:设 A 为离心率为 2 的双曲线的一支的顶点,S 为其另一支的焦点.以 AS 为弦作一圆弧使所含角③为已知角的补角.设此圆弧与双曲线的过 S 的一支交于点 P.则 PAS 即等于已知角的三分之一.

克莱罗解法 下边一个漂亮的解法是克莱罗④(Clairaut)提出的.设 AOB 为已知角.取 $OA=OB$,以 O 为中心并以 OA 为半径作圆.连 AB,并三等分之,设分点为 H 及 K,于是 $AH=HK=KB$.以 A 为焦点,H 为顶点,OC 为准线作一双曲线.设此双曲线过 H 的一支和圆交于点 Q.则由顶点与准线的性质可知 $AP:PM=AH:HL=2:1$,于是 $AP=2\cdot PM=PQ$.因此据对称性得 $AP=PQ=QB$.所以 $AOP=POQ=QOB$.

---

① Geometria,卷Ⅲ,Schooten 出版,Amsterdam,1659,p.91.

② Arithmetica Universalis,问题 XLII,Ralphson 第 2 版,London,1728,p.148;又,pp.243—245.

③ 指圆心角.——译者注

④ 我相信这是克莱罗(Clairaut)首先提出的,但是我把参考资料失落了.这个作图法作为一个例子出现于 C. Taylor 的 Geometry of Conics (Cambridge,1881,no. 308,p.126)里.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

[346] **沙勒解法** 最后我要给出沙勒(Chasles)[①]认为是最基本的解法.它和下边的命题是等价的.设 OA 与 OB 是达于圆弧 AB 两端的两个半径,圆的点 A 处的切线和 OB 的延长线的交点为 P,则以 OA 为实轴而过 P 的正双曲线必过圆弧 AB 的三等分点之一.

已经造出几种仪器,利用它可以把已知角三等分.

化 圆 为 方[②]

三个古典问题的第三个是求正方形的边长,要此正方形的面积须等于已知圆的面积.

多少世代以来,这个问题的研究不仅引起数学家们的极大兴趣,而且也常使一般人感到非常有趣.事实上,错误证明的出现竟那么多,使得巴黎科学院1775年不得不作出一决定,声明不再检验化圆为方问题的解法.虽然如此,这个问题的钻研却发现了许多有关定理.近代,了解问题本质的人都把它放弃了.权威的作者们已经写出了这个问题的详细历史,所以我在这里只打算简略地提一提.

阿基米德证明过[③](可能先前已为人所知),这个问题等价于要求一个直角三角形的面积,它的直角边分别等于圆的周长
[347] 和半径.这两个线段的比值的一半通常记为 π.

兰伯特(Lambert)于1761年证明了此数的无理性[④];他证

① Traité des sections coniques, Paris, 1866, art. 37. p.36.

② 参看 Montucla's Histoire des Recherches sur la Quadrature du Cercle, edited by P.L. Lacroix, Paris, 1831;以及 A. De Morgan 的许多文章,特别是他的 Budget of Paradoxes, London, 1872.舒伯特(H. Schubert)曾编纂过一本关于这个问题的通俗小册子:Die Quadratur des Zirkels, Hamburg, 1889;自从这些"消遣品"的早期出版问世后,苏黎世(Zurich)的鲁迪奥(F. Rudio)教授曾对阿基米德、惠更斯、兰伯特(Lambert)与勒让德关于这个问题的论述作过一个分析,并附有此问题的历史概述.Leipzig, 1892.

③ Archimedes Opera, Κύκλου μέτρησις, 命题Ⅰ, Torelli 出版, pp.203—205;Heiberg 出版,卷Ⅰ, pp.258—261,卷Ⅲ, pp.269—277.

④ Mémoires de l'Academie de Berlin for 1761, Berlin 1768, pp.265—322.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

明：若 $x(\neq 0)$ 为有理数，则 e^x 与 $\tan x$ 都不可能是有理数. 而 $\tan\left(\frac{1}{4}\pi\right)=1$；所以 $\frac{1}{4}\pi$ 必为无理数，因而 π 为无理数.

π 的超越性是 1882 年林德曼（Lindemann）证明的①. 他先证明：若 x 为某整有理代数方程的一个根，则 e^x 不可能是有理数. 于是，若 πi 是某整有理代数方程的根，则 $e^{\pi i}$ 不可能是有理数. 但 $e^{\pi i}=-1$，这是个有理数，所以 πi 不可能是整有理代数方程的根，因而 π 也不可能是.

较早些时候，杰姆斯·格雷戈里（James Gregory）②曾试图证明化圆为方是不可能的，但他的证明未能令人信服.

如果 π 仅仅表示圆周与直径之比，那么不待言求它的数值是没有多大趣味的. 但是，不幸通常 π 的定义正是那样说的. 事实上，它表示那样一个数，不论从哪一方面探讨分析这一数学分支时它都是要出现的. 一个典型的例子是方程 $e^{\pi i}+1=0$. 实际上，圆周长度与直径长度之比值为 π 这件事实并没有给 π 提供最好的解析定义而只不过是 π 的一个性质. 我想起来有一位著名的教授曾讲解过，如果有一种生命，他们生活中的算术、代数、几何法则和我们看来是显然的那些法则不同的话，那么他们的日常生活在我们看来将会是多么奇特. 但是他又说，无法想象一种宇宙其中竟不存在 e 和 π.

符号 π 的来源

用 π 这个符号表示 3.141 592 653 589 793 238 462 643 383 279 502 884 197 169 399 375 105 820 974 944 592 307 816 406 286 208 998 628 034 825 342 117 067 9 …这个数可以追溯到 1647 [348]
年，那时奥特雷德用 δ/π 表示直径与圆周之比；1697 年格雷戈

---

① Uber die Zahl π, Mathematische Annalen, Leipzig, 1882, Vol. XX, pp. 213—225.

② Vera Circuli et Hyperbolae Quadratura, Padua, 1668；此文转载于惠更斯的 Opera Varia, Leyden, 1724, pp. 405—462.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

里用 π/ρ 表示圆周与直径之比.单独使用 π 这个符号大约开始于 18 世纪初.威廉·琼斯(William Jones)①于 1706 年用 π 表示上述比值,数年之后②,约翰·伯努利(Johann Bernoulli)用 c 表示它.欧拉于 1734 年用 p,又于 1736 年用 c;哥德巴赫(C. Goldbach)于 1742 年用 π;从欧拉的"分析"一书出版后,π 这个符号才普遍地被采用.

π 的数值可以用下述两种方法之一求之,其精确程度可以达到任意指定的高度.

第一个方法是几何的方法,即,计算一个圆的内接正多边形的周长和外切正多边形的周长,并假定圆的周长介于两者之间.③如果通过计算面积而不是计算周长而求 π 的数值,结果会更精确些.第二个方法就是现代的方法,它先寻求表示 π 的收敛的无穷级数,再计算级数的近似和而得到 π 的近似值.

可以说,采用第一种方法的 π 计算者们是把 π 看成一个几何量的比,而采用第二种方法的 π 计算者们是把 π 看成表示一个定数的符号,这个数进入到数学分析的许多分支里.

在这里附上各个作者所给的 π 的近似值④会是有趣的.顺

---

① Synopsis Palmariorum Matheseos, London, 1706, pp.243, 263.

② 参看 Bibliotheca Mathematica, Stockholm, 1889, Vol. Ⅲ, p.28;又,1890,Vol. Ⅳ, p.22 上恩内斯特勒姆(G. Eneström)所写的注记.

③ 塞兰德(K. E. I. Selander)在他的 Historik öfver Ludolphska Talet (Uspala, 1868)里写了这个方法的历史.

④ 关于古代所用方法及其结果,参看康托尔(M. Cantor)的 Geschichte der Mathematik (Leipzig, Vol. Ⅰ, 1880)里关于那些作者的注记.关于中世纪和近代的逼近法,参看 Penny Cyclopaedia (London, 1841) Vol. XIX 里由德摩根所写关于化圆为方的条目;以及在阿姆斯特丹的 Verhandelingen (1858, Vol. Ⅳ, p.22)里德哈恩(D. de Haan)所写的补充;格莱谢尔将各种结果列表:校正并予扩展,载于 Messenger of Mathematics, Cambridge, 1873, Vol. Ⅱ, pp.119—128;又,1874,Vol. Ⅲ, pp.27—46.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

便也就指出那些研究这个问题很有成绩的人. [349]

求 π 的近似值的几何方法

埃及人①在公元前 1700 年前后取 256/81 作为 π 的近似值;这个分数等于 3.1605…;但巴比伦人②和犹太人③则用更粗略的近似值 3. 这些数字很可能是从经验得来的.

往后是一长串研究这个问题的希腊数学家的名单. 约恩(Ionian)学派、毕达哥拉斯(Pythagoras)学派、安纳克萨戈拉斯(Anaxagoras)、希皮亚斯(Hippias)、安蒂福(Antipho)以及布赖索(Bryso)是否导出过 π 的近似值是可疑的,我们也不必耽搁在他们的研究上. 希俄斯(Chios)的希波克拉蒂斯化某些弓形为方是很机敏的,也是正确的,但不能从其中得到 π 的值. 似乎雅典学派的晚辈都把他们精力集中到其他问题上去了.

亚历山大学派杰出的奠基人欧几里得④很可能觉察到了 π 大于 3 而小于 4,但他不曾明确叙述过这个结果.

这个问题的数学处理始于阿基米德,他证明了 π 小于 $3\frac{1}{7}$ 而大于 $3\frac{10}{71}$,即,介于 3.1428…和 3.1408…之间. 其证法是⑤给一个圆作内接正 96 边形和外边正 96 边形,然后用几何的方法求这两个正多边形的周长,最后再假定圆的周长介于这两个多边形的周长之间. 这样就得到了上边所说的两个界限. 这个方法等价于利

① Ein mathematisches Handbuch der alten Aegypter(即莱茵德莎草纸书),艾森洛尔(A. Eisenlohr)编,Leipzig, 1877, 第 100—109 节,117 节及 124 节.

② Oppert, Journal Asiatique, August 1872; October 1874.

③ 1. 金斯(Kings)第 7 章第 23 节;2. 克朗尼克尔斯(Chronicles)第 4 章,第 2 节.

④ 这些结果可由"原本"卷Ⅳ,15 与 8 推出;又见卷 XII,命题 16.

⑤ Archimedes Opera, Κύκλου μέτρησις, 命题Ⅲ, Torelli 版, Oxford, 1792. pp.205—216; Heiberg 版, Leipzig, 1880, 卷Ⅰ, pp.263—271.

我们必须知道,而且我们必将知道


[redacted]

用命题 $\sin\theta<\theta<\tan\theta$，$\theta=\pi/96$. 阿基米德通过重复平分一个角度为 $\pi/3$ 的角而推出了 $\sin\theta$ 和 $\tan\theta$ 的值. 如果采用正 n 边形，则这个方法将推出 π 的一个近似值，其小数点后的可靠位数
[350] 至少达到 $2\log n-1.19$ 的整数部分. 阿基米德的结论的小数点后只有头两位是正确的. 他的分析得出这样一个论断：如果圆的直径是 4 970 呎，那么它的内接、外接正 96 边形的周长介于 15 610 呎和 15 620 呎之间；此圆的真正周长约等于 15 613 呎 9 吋.

阿波罗尼奥斯讨论过这些结果，但他的评议已经失传.

亚历山大里亚的希罗给出①近似值 3，但他引用过②22/7. 前者可能是他有意取的粗略近似值.

我要说的仅有的另一个希腊近似值是托勒密（Ptolemy）③所给出的近似值，他断言 $\pi=3°8'30''$. 这等于取 $\pi=3+\frac{8}{60}+\frac{30}{3600}=3\frac{17}{120}=3.1416$.

罗马的测量员似乎曾用过 3，有时候或者用 4 作粗略的计算. 他们作精确的计算时用 $3\frac{1}{8}$ 而不用 $3\frac{1}{7}$，因为前一个分数在十二进位制的算术里更为方便. 另一方面，热尔贝（Gerbert）④（大约公元前 1000 年）推荐采用 22/7.

在谈到中世纪的和近代的欧洲数学家之前，应该提到印度和东方数学家取得的成就.

印度数学家的成就

鲍德海雅纳⑤（Baudhayana）取 49/16 作为 π 的近似值.

---

① Mensure, ed. Hultsch, Berlin, 1864, p.188.

② Geometria, ed. Hultsch, Berlin, 1864, pp.115, 136.

③ Almagest，卷Ⅵ，第 7 章；ed. Halma. 卷Ⅰ, p.421.

④ Œuvres de Gerbert, ed. Olleris, Clermont, 1867, p.453.

⑤ 蒂博（G. Thibaut）著：The Sulvasutras, Asiatic Society of Bengal, 1875，第 26—28 节.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

圣使阿耶波多①(Arya-Bhata)大约于公元530年给出62382/20000,这等于3.1416.他证明了:若单位圆的内接正n边形的边长为a,内接正$2n$边形的边长为b,则$b^2=\frac{1}{2}-\frac{1}{2}(1-a^2)^{1/2}$.从内接正6边形算起,他算出了正12边形,正24边形,正48边形,正96边形,正192边形以及正384边形的边长.最后这个正多边形的周长是$\sqrt{9.8694}$,取近似的平方根而得到他的结果.

婆罗摩笈多(Brahmagupta)②于公元650年左右给出$\sqrt{10}$, [351]
它等于3.1622….据说他在单位圆内作边数为12,24,48和96的正多边形,依次求出了它们的周长为$\sqrt{9.65}$,$\sqrt{9.81}$,$\sqrt{9.86}$,$\sqrt{9.87}$,于是他假定了当边数无限增多时,周长大约等于$\sqrt{10}$.

巴斯卡拉(Bhaskara)大约于公元1150年给出两个近似值.一个③(可能是从阿耶波多那里抄来后又重新用阿基米德的方法计算了正384边形的周长)是3927/1250,这等于3.1416.

中国数学家的成就

中国的天文学家祖冲之(生于公元430年)④证明了π的值介于3.1415926和3.1415927之间,并从而导出他所称的"密率",355/113.

阿拉伯数学家的成就

在阿拉伯人中,阿尔·卡西(J. M. al Kashî)(1436年左右)得到2π的近似值6.2831853071795865.它的小数点后的16位数字都是正确的.这个数是从他先前算得的一个六十进位的9位数转换成的.它使他保持着直到1596年的世界纪录.此

---

① 罗德(L. Rodet)著文 Leçons de calcul d'Aryabhata,载于 the Journal Asiatique, 1879, series, 7, Vol. XIII, pp.10,21.

② Algebra ... from Brahmeguta and Bhascara,科尔布鲁克(H. T. Colebrooke)译,London, 1817,第XII章,第40节,p.308.

③ 同上,p.87.

④ E. W. Hobson, Squaring the Circle, Cambridge, 1913, p.24.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

外，这也几乎可以肯定是对一个分数进行基数转换的第一个例子①.

欧洲数学家的成就

转来谈欧洲的数学家们.这里有下边的 π 的一系列的近似值，其中许多是早在 18 世纪之前着眼于证实某些有关的求积的错误而计算的.

比萨(Pisa)的莱昂纳多(Leonardo)②在 13 世纪给出了 π 的近似值 $1\,440/458\frac{1}{3}$，它等于 3.141 8…. 15 世纪中，普尔巴赫(Purbach)③给出或者是引用过 62832/20000，它等于 3.1416. 库萨(Cusa)
[352] 相信 π 的精确值是 $\frac{3}{4}(\sqrt{3}+\sqrt{6})$，它等于 3.1423…；据说 1464 年雷格蒙塔努斯(Regiomontanus)④给出过一个近似值 3.14243.

韦达⑤于 1579 年证明了 π 大于 $31\,415\,926\,535/10^{10}$ 而小于 $31\,415\,926\,537/10^{10}$. 这个结果是重复应用公式 $2\sin^2\frac{1}{2}\theta=1-\cos\theta$ 于计算内接正 6×2^{16} 边形和外切正 6×2^{16} 边形的周长而得到的. 他还给出⑥过一个和下列公式等价的结果：

$$\frac{2}{\pi}=\frac{\sqrt{2}}{2}\,\frac{\sqrt{2+\sqrt{2}}}{2}\,\frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}\cdots.$$

---

① D. E. Knuth, The Art of Computer Programming, Vol. Ⅱ, Reading, Massachusetts, 1969, pp.165—167.

② Boncompagni's Scritt di Leonardo, Vol. Ⅱ (Practica Geometriae), Rome, 1862, p.90. Leonardo 外号是斐波那契 Fibonacci(见本书第 57 页).

③ 雷格蒙塔努斯的 De Triangulis 的附录，Basle, 1541, p.131.

④ 见于他致库萨的尼古拉斯(C. Nicholas de Cusa)的通信，De Quadratura Circuli, Nuremberg, 1533, 其中他证明了尼古拉斯的结果是错误的.我未能引述确切的资料，但这些数字是权威的作者们给出的，我不怀疑其正确性.

⑤ Canon Mathematics seu ad Triangula, Paris, 1579, pp.56,66.这个著作可能是为了私下交流而印的，极为少见.

⑥ Vietae Opera, ed. Schooten, Leyden, 1646, p.400.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

梅蒂尤斯(A. Metius)①之父于1585年给出355/113,它等于3.14159292…,小数点后前六位是正确的.这是一个奇特而幸运的猜想,因为他只证明了π介于377/120和333/106之间,然后就跳到他的论断说将这两个分数的分子与分母各取算术平均值则所得新的分数就是π.

罗曼努斯(A. Romanus)②于1593年计算了内接正1 073 741 824(即2^{30})边形的周长,从而得到正确到小数点后前15位的π值.

范·雪伦(L. van Ceulen)一生大部分时间致力于这个问题.1596年③他给出一个20位小数的结果,那是通过求内接的和外切的正60×2^{33}边形的周长而得到的.他重复利用了自己发明的 [353]
和$1-\cos A=2\sin^2\frac{1}{2}A$等价的公式.我藏有他的一幅签字的木刻版画,在他的肖像下边的一个圆的周围印着这个结果.氏死于1610年,遵照遗嘱,在莱登(Leyden)圣彼得教堂里他的墓碑④上刻有35位小数的近似值(那是他计算出的位数最多的结果).他的算术遗著⑤里载有32位的结果,那是他通过计算一个正2^{62}即4 611 686 018 427 387 904边形的周长而得到的.范·雪伦还编制了一个各种正多边形周长的表.

---

① Arithmeticae libri duo et Geometriae, 梅蒂尤斯著, Leyden, 1626, pp.88—89.〔可能原先出版于1611.〕

② Ideae Mathematicae, Antwerp, 1593;稀缺之书,我从未能查阅过.

③ Van den Cirkel, Delft, 1596,对开卷14,p.1;或De Circulo, Leyden, 1619, p.3.

④ 德哈恩教授在Messenger of Mathematics, 1874, (N.S.) Vol. Ⅲ, p.25上引述过这个铭刻.

⑤ De Arithmetische en Geometrische Fondamenten, Leyden, 1615, p.163;或斯内尔的拉丁文译本Fundamenta Arithmetica et Geometrica, p.144, 1615年出版于Leyden.此书于1619年又和Van den Circkel的拉丁译文合订出版,书名是De Circulo,参看其中pp.3,29—32,92.

我们必须知道，而且我们必将知道

斯内尔(Willebrord Snell)①于1621年从一个正2^{30}边形得到一个有34位小数的近似值.这比范·雪伦所给的位数少,但斯内尔的方法优越得多,采用同样的正多边形而计算时,他得到34位而范·雪伦仅得到14(或许是16)位.类似地,斯内尔从一个六边形得到的近似值和阿基米德需要从96边形才能得到的近似值有同样的精确度,而用96边形时他得的π的近似值的小数点后前七位数字都是正确的,阿基米德得的结果却只有两位正确数字.原因在于,阿基米德在计算了内接正n边形的边长和外切正n边形的边长之后,假定圆周长的$1/n$介于二者之间;而斯内尔根据这两个边长作出了另外两个线段,它们给出了所夹弧的更精确的界限.他的方法的基础是这样一个定理:$3\sin\theta/(2+\cos\theta)<\theta<\left(2\sin\frac{1}{3}\theta+\tan\frac{1}{3}\theta\right)$.根据这个定理,一个正$n$边形所给$\pi$的近似值的小数部分可靠数字的位数至少等于$(4\log n-0.2305)$的整
354] 数部分,这要比旧的方法所给的位数至少多一倍.斯内尔对他的定理的证明是错误的,不过结论是对的.

斯内尔也造过一个表②,表中列出边数为10×2^n的所有内接正多边形的周长和外切正多边形的周长,n从3到19.表值大部分是从范·雪伦那里摘引来的,但有些是他重新计算过的.这个表在驳斥化圆为方家们时起过作用.格雷戈里③也造过一个同类的表.

1630年格林伯格(Grienberger)④借助于斯内尔的定理把π的近似值计算到小数点后39位.他是采用求内接、外切正多边形周长的古典方法的最后一位数学家.更精确的近似值没有什

① Cyclometricus, Leyden, 1621, p.55.

② 蒙蒂克拉曾引用过,1831年出版,p.70.

③ Vera Circuli et Hyperbolae Quadratura,命题29,惠更斯引用于Opera Varia, Leyden, 1724, p.447.

④ Elementa Trigonometrica, Rome, 1630,序言末尾.

http://maths352.bokee.com

么实用价值.惠更斯在一篇文章[①]中给出了斯内尔和其他计算者们采用这个方法时所据定理的证明,可以认为该文结束了古典方法的历史.

求 π 的近似值的分析方法

1656 年沃利斯(Wallis)[②]证明了

$$\frac{\pi}{2}=\frac{2}{1}\,\frac{2}{3}\,\frac{4}{3}\,\frac{4}{5}\,\frac{6}{5}\,\frac{6}{7}\,\frac{8}{7}\cdots,$$

并据布龙克尔(Viscount Brouncker)数年前给出的一个命题而得到

$$\frac{4}{\pi}=1+1^2/2+3^2/2+5^2/2+7^2/\cdots,$$

但是这两个定理都未曾被广泛应用于计算.

1699 年—1873 年间欧洲人的结果

后来的计算者都依靠收敛的无穷级数去进行计算.在微积 [355]
分发明之前,这种方法是很难实行的,纵然笛卡儿[③]曾指出过一个和无穷级法是等价的几何步骤.无穷级数的采用是格雷戈里提出的[④],他证明了:当且仅当 $-\frac{1}{4}\pi<\theta<\frac{1}{4}\pi$ 时

$$\theta=\tan\theta-\frac{1}{3}\tan^3\theta+\frac{1}{5}\tan^5\theta-\cdots.$$

---

① De Circula Magnitudine Inventa, 1654; Opera Varia, pp.351—387. 证明载于皮里(G. Pirie)的 Geometrical Methods of Approximating to the Value of π, London, 1877, pp.21—23.

② Arithmetica Infinitorum, Oxford, 1656, 命题 191.凯莱写过一篇这种研究的分析,见 Quarterly Journal of Mathematics, 1889, Vol. XXIII, pp.165—169.

③ 参看欧拉的文章,载于 Novi Commentarii Academiae Scientiarum, Petrograd, 1763, Vol. Ⅷ, pp.157—168.

④ 见致科林斯(Collins)的信,Feb. 15, 1671,载于 Commercium Epistolicum, London, 1712, p.25,又见麦克尔斯菲尔德(Macclesfield)文集,Correspondence of Scientific Men of the Seventeenth Century, Oxford, 1841, Vol Ⅱ, p.216.

我们必须知道,而且我们必将知道

http://maths352.bokee.com

第一位利用J·格雷戈里的级数去求 π 的近似值的数学家是夏普(Abraham Sharp)①，1699年，他按照哈雷(Halley)的建议，确定了 π 的72位小数(71位是正确的)．他在格雷戈里的级数里取 $\theta=\frac{1}{6}\pi$ 而得到这一结果．

梅欣②(Machin)在1706年之前，给出了100位的结果(全部正确)．他是用下列公式计算的：

$$\frac{1}{4}\pi=4\tan^{-1}\frac{1}{5}-\tan^{-1}\frac{1}{239}.$$

德·拉尼(de Lagny)③在1719年把结果给算到小数点后127位(112位正确)，也是将 $\theta=\frac{1}{6}\pi$ 代入格雷戈里的级数里而计算的．

赫顿④在1776年、还有欧拉⑤在1779年，都建议用公式 $\frac{1}{4}\pi=\tan^{-1}\frac{1}{2}+\tan^{-1}\frac{1}{3}$ 或 $\frac{1}{4}\pi=5\tan^{-1}\frac{1}{7}+2\tan^{-1}\frac{3}{79}$，但他们都不曾
[356] 算到比前人更多的位数．

维伽(Vega)⑥在1789年把 π 的值给到143位(126位正

---

① 参看卡德沃斯(W. Cudworth)著 Life of A. Sharp, London, 1889, p.170. 在舍温(Sherwin)的 Mathematical Tables 的前边(53页以后)给出了夏普的浅谈．此表出版于1705年，可能"浅谈"是同时出版的．不过我见到的最早的版本是1717年印刷的．

② W. Jones's Synopsis Palmariorum, London, 1706, p.243; Maseres, Sciptores Logarithmici, London, 1796, Vol. Ⅲ, pp. vii—ix, 155—164.

③ Histoire de l'Academie for 1719, Paris, 1721, p.144.

④ Philosophical Transactions, 1776, Vol. LXVI, pp.476—492.

⑤ Nova Acta Academiae Scientiarum Petropolitanae for 1793, Leningrad, 1798, Vol. Ⅺ, pp.133—149；此文1779年宣读．

⑥ Nova Acta Academiae Scientiarum Petropolitanae for 1790, Lenigrad, 1795, Vol. Ⅸ, p.41.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

确);又在 1794 年给到 140 位(136 位正确).

18 世纪末,冯·察赫(F.X. von Zach)在牛津的拉德克利夫(Radcliffe)图书馆里看到了一位不知名作者的一份手稿中给出了 π 的 154 位小数(152 位是正确的).

1837 年出版了 π 值的一个计算结果,到 154 位小数(152 位正确)①.

1841 年卢瑟福(Rutherford)②利用公式

$$\frac{1}{4}\pi = 4\tan^{-1}\frac{1}{5} - \tan^{-1}\frac{1}{70} + \tan^{-1}\frac{1}{99}$$

把 π 计算到 208 位小数(152 位正确).

1844 年达泽(J.M.Z. Dase)③利用公式

$$\frac{1}{4}\pi = \tan^{-1}\frac{1}{2} + \tan^{-1}\frac{1}{5} + \tan^{-1}\frac{1}{8}$$

把 π 计算到 205 位小数(200 位正确).

1847 年克劳森(Clausen)④分别用两个公式

$$\frac{1}{4}\pi = 2\tan^{-1}\frac{1}{3} + \tan^{-1}\frac{1}{7}$$

和

$$\frac{1}{4}\pi = 4\tan^{-1}\frac{1}{5} - \tan^{-1}\frac{1}{239}$$

把 π 的近似值算到 250 位(248 位正确).

1853 年卢瑟福⑤把他先前的结果推进到 440 位小数(全部正确),尚克斯(William Shanks)又把这近似值延伸到 530 位

---

① J. F. Callet's Tables, etc., Précis Élémentaire, Paris, tirage 1837. Tirage 1894, p.96.

② Philosoplical Transections, 1841, p.283.

③ Crelle's Journal, 1844, Vol. XXVII, p.198.

④ Schumacher, Astronomische Nachrichten, Vol. XXV, col. 207.

⑤ Proceedings of the Royal Society, Jan. 20, 1853, Vol. VI. pp. 273—275.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

[357] (527 位正确)①.以后的二十年中尚克斯企图再向前挺进,但是他在第 528 位小数上的错误使后来的一切数字都无效了②.

1853 年,黎赫特(Richter)可能对英国的工作无所了解,求出了 π 的 333 位③小数(330 位正确);1854 年他又把这个近似值推进到 400 位④,1855 年又推进到 500 位⑤.

用以计算这些近似值的级数与公式中,以梅欣与达泽所用者恐怕要算是最简便的了.其他收敛较快的级数有

$$\frac{\pi}{6}=\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{3\cdot 2^3}+\frac{1\cdot 3}{2\cdot 4}\cdot\frac{1}{5\cdot 2^5}+\cdots,$$

$$\frac{\pi}{4}=22\tan^{-1}\frac{1}{28}+2\tan^{-1}\frac{1}{443}-5\tan^{-1}\frac{1}{1393}-10\tan^{-1}\frac{1}{11018}+\cdots.$$

后一个是埃斯科特(E. B. Escott)⑥先生推出的.

有一个可悲的讽刺,认为这种占去了可怜的尚克斯先生大半生的计算现在可以用几秒钟去重复一遍(不去重复他那巨大的错误),好"温一温"电子计算机.

至于那些自认为已经化圆为方了的作者们大军,他们中大多数极为无知,其尝试在此不值一谈.有人说"你走你的阳关道,我过我的独木桥!"令人一叹!无疑,"化圆为方"这个命题对人们的魅力实在是太大了!

---

① Contributions to Mathematics, W. Shanks, London, 1853, pp.86—87.

② D. F. Ferguson, Nature, March, 1946, Vol. CLVII, p.342.

③ Grünert's Archiv, Vol. XXI, p.119.

④ 同上,Vol.XXIII, p.476;在 Vol.XXII 里 p.433 上所载的近似值只有 330 位是正确的.

⑤ 同上,Vol.XXV, p.472;又见于 Elbinger Anzeigen No.85.

⑥ 关于此类公式的详尽讨论,请参看 John Todd, American Mathematical Monthly, 1949, Vol. LVI, pp.517—528.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

在拟似真值的几何方法中，以下边的一个最为简单．在给定 [358]
的圆内作内接正方形，将此正方形的一边长的五分之一和直径的三倍相加，所得结果与此圆周长的差小于圆周长的一万八千分之一．

根据概率理论求 π 的近似值

在一个平面上画一些间距为 a 的平行线．取长度为 $l(<a)$ 的一只小棍，掷于平面上．小棍跨压一条直线的概率是 $2l/\pi a$．如果将此试验重复几百几千次，则有利情况数与试验总数之比将与这个分数十分接近，从而可以求出 π 的值．1855 年，阿伯丁(Aberdeen)[①]的史密斯先生做过3204次试验，得到 $\pi=3.1553$．德摩根教授[②]的一位学生用 600 次试验得到 $\pi=3.137$．1864 年，福克斯上尉(Captain Fox)[③]格外细心地做了 1120 次试验，得到近似值 $\pi=3.1419$．

还提出过求 π 的近似值的其他类似的方法．例如，大家知道如果随便写下两个数字，那么它们互质的概率是 $6/\pi^2$．据此，有一次[④]曾有 50 个学生各自随机地写下 5 对数字，发现其中有 154 对是互素的．于是 $6/\pi^2=154/250$，由此得到 $\pi=3.12$． [359]

---

① Aberdeen 为美国华盛顿州西部一港口．——译者注

② A. De Morgan, *Budget of Paradoxes*, London, 1872, pp.171,172.

③ *Messenger of Mathematics*, Cambridge, 1873, Vol. Ⅱ, pp.113, 114.关于福克斯上尉的一篇有趣的“格外细心”(additional precautions)和用这种方法获得真正好的近似值的不可能性，可参看奥贝恩(T. H. O'Beirne)著 *Puzzles and Paradoxes* (London, 1965)第 195—197 页上的一节“好得难以置信?”(Too good to be true?)

④ 沙特尔(R. Chartres)著 Note on π，载于 *Philosophical Magazine*, London, Series 6, Vol. XXXIX, March, 1904, p.315.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第13章 心算神童

天赋有非凡心算能力的儿童旷世罕见①.他们能在几秒钟内回答出关于大数相乘或开方问题的结果,而专门的数学家要借助于笔和纸在长时间内才能得出那些答案来.他们的能力并非总是限于回答那种简单的问题.许多难题,例如关于分解因子、复利、年金、民历与教会历以及解方程等,一旦他们理解了问题的要求,有些人就轻而易举地立即给出解答.这些孩子们大多数没有受什么教育,而且他们所用的方法通常都是自己发明的.

他们的表演是那么卓绝,使得有些观众认为那些神童具有非凡的本领.这种观点是没有根据的.任何一个记忆力强而又爱好算术的孩子,如果他专心致志于数学而能持之以恒,都能练出

[360] 优异的心算能力.当然,那些天资特好者的表演是特别惊人的.

在这一章里,我打算简述一下那些较著名的心算神童们的事迹.将会看到,他们的表演性质大体上相同,不过程度有所差异.所以,对于后边的那些人,只须简要地指出不同心算者的特

① 关于心算神童的大部分事迹都有收集.参看 E. W. Scripture, American Journal of Psychology, 1891, Vol. N, pp.1—59; F.D. Mitchell, 同刊 1907, Vol. XVIII, pp.61—143; G. E. Müller, Zur Analyse der Gedächtnistätigkeit und des Vorstellungsverlaufes, Leipzig, 1911.我随意引用了这些文章,在我没有第一手资料而引述某些权威的情况下,就完全依靠它们.关于众多的原始权威的索引应查询这些文章.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

点就够了.

我只谈那些自学成才的心算者,而那些通过演习、算术上的安排和表演主持人的诡计而装成天赋似的个别表演者则不予记述.我还只谈那些在青少年时代显露出这种天赋的人.就我所知,我这样排除不论的年长后自学成名的数学家只有一个**约翰·沃利斯**教授(1616—1703),牛津的萨维勒人.出于自娱,他在中年时期发展了他的心算能力.作为他的成就的一个例子,我举出 1669 年 12 月 22 日他尚未起床时心里在想求 3×10^{40}的平方根的整数部分,几个小时后,他据记忆写下了结果.这件事引起了注意,两个月后,有人向他挑战比赛心算开一个 53 位数的平方,当时未曾把它写下来.过了一个月,他又背出了答案.这样的心算和记忆成果是心算神童们事迹的典型.

有案可查的最早的神童之一是**朱迪代亚·巴克斯顿**(Jedediah Buxton),1707 年生于英国德比郡(Derbyshire)的埃尔姆顿(Elmton).虽然是一位乡村小学校长的儿子,可是未曾上学,从未学过写字和数码.除了天生会算大数以外,他的智力是很低的.他没有什么雄心,一生干农活.他的计算特长没有给他带来任何物质利益,除了偶尔从邀请他去表演的主持人那里得到一点小钱.他死于 1772 年.

他不记得何时或何以他开始对心算发生了兴趣.关于他早年 [361]
的表演也无史料可考.无论如何,他对于单纯的数字总是像有一种奇特的魔力似的.如果告诉他一个物体的大小,他立即就算出是几吋长或多少根头发丝那么宽;如果告诉他一段时间,他立即算出是多少分钟;如果他去听一课布道,他想的只是一共说了几个字或多少音节.无疑,由于不断的练习,他在这方面的能力也不断地增加;但是他的头脑是很幼稚的,似乎不过为自己能够准确地说出此类计算的结果而自满.他的智力迟钝,比起别的神童来,在回答算术问题时要缓慢得多.他的特长在实际问题上取得的仅有的成就是能够凭观察而估计出一块形状不规则的土地的亩数.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

他的名声逐渐传遍了德比郡.下边是当地来访者提的许多问题中的一些,它们足以表明这个年轻人的能力.一块351码长,261码宽的土地的面积有多少亩? 11分钟内答出.要掘一个426呎长,263呎宽,2 $\frac{1}{2}$呎深的池塘,须运走多少立方码的土? 15分钟内答出.假定声音每秒钟传播1 142呎,问多长时间才能传5哩? 15分钟内答出.这类问题不含有原理上的困难.

下边是巴克斯顿的能力达到顶峰时解答的几个较难的问题.他算出了把一个法星①翻140翻是多少钱.这个答数以镑计需要39位数字表示,外加零头2先令8便士.后来又问他这个39位数自乘一次是多少? 两个半月后他给出了答数,他说是在两个半月内断断续续地算出来的.1751年他算出了一块23 145 789码长,5 642 732码宽,54 965码高的长方块里有多少立方吋;体积为202 680 000 360立方哩的立方谷仓,要装满它需
[362] 要多少喱②谷物? 又问装满它需要多少根一吋长的头发?——一喱谷物的体积和头发的粗细都给出了.这些问题涉及的数字都是极其巨大的,但问题的本质并不困难,然而,除非计算者具有非凡的记忆力,否则是无法心算的.他每次给出的答案都是正确的,虽然要花不少的气力才答得出来.1753年有人要他算出一个正立方形斗的大小,这斗恰好能装一夸特③麦.他认识到回答这个问题需要一种和开立方等价的算法,对于他来说这是一个新的概念,不过在一个钟头内他还是说出了那个斗的棱长在25 $\frac{1}{2}$吋和26吋之间,这是对的.估计他是试算了许多数字而得到这个答案的.

表演被报导了,于是其声誉传播到伦敦.1754年他走访伦

① 一法星(farthing)等于四分之一便士.——译者注

② 一喱(grain)等于七千分之一磅.——译者注

③ 1夸特(Quarter)=28磅.——译者注

我们必须知道，而且我们必将知道

敦，受到皇家学会会员们的考验．表演的真实性得到确认．他的几位熟人带他去特鲁利街（Drury Lane）某剧院去看伽立克（Garrik）的演出，他们怀着好奇心想看看他对戏剧有何种感受．不料出了剧院他向东道主谈的却是各个演员嗓子里发出的字音数目和另一些演员各人舞蹈的步子的数目，对于剧情则毫无感受．

只有在极少见的情况下，他能够解说他所采用的算法，不过，知道他那些解释后，我们已足可判定其算法是很笨拙的了．他解释他计算 456 乘 378 的办法是（用我们的话来简单地说）：用 a 表示前一个数，他先算出 $5a=$（譬如说）b，然后算出 $20b=$（譬如说）c，再算算出 $3c=$（譬如说）d；然后他又去计算 $15b=$（譬如说）e，再把它加到 d 上；最后算 $3a$，把它加到刚才的结果上而得出答数．这等于说他把乘数 378 折成 $(5\times20\times3)+(5\times15)+3$．米切尔（Mitchell）认为这意味着巴克斯顿是用 60 与 15 的倍数去进行计算，然后化乘法为加法．事情可能是这样，因为难以设想他不明白用 5 和 20 连乘等于用 100 乘一次，这结果是 [363]
立即可知的．他从未听到过亿①、兆之类的大数单位名称，为了表达向他提的问题中涉及的特大数字，他设立了一些自己用的单位，把 10^{18}叫做一簇（tribe），把 10^{36}叫做一箍（cramp）．

像一切这些计算者一样，他的记忆力特殊地好，随着时日的推移，他记住了许多数字（如某些经常遇到的某些数的乘积，一年里有多少分钟，一英里等于多少根头发的宽），这些记忆又大大加快了他的计算．他的一个奇异的也许是唯一的特点是能在心算的中途随时暂停下来去干别的事，过一会儿或者几个星期后接着再算下去．他还能回答两个或多个同时提出的比较简单的问题．

18 世纪的另一个神童是**托马斯·富勒**（Thomas Fuller），他是

① 原文 billions 为十亿，但意在强调单位名称，故改用亿．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

1710年出生于非洲的黑人.1724年他在那里被绑架当作奴隶转卖到美国弗吉尼亚(Virginia)州,生活在那里直到1790年去世.和巴克斯顿一样,富勒从未学读书或写字,他的能力只限于心算.他能心算两个九位数的乘积,说出指定时间内的秒数,一定量谷物的粒数,等等.总之,能回答通常向神童们提的老一套问题,但要限于只涉及需用乘法和用比例去解决的问题.虽然比巴克斯顿算得快一些,但比起下边所说一些神童仍是一个慢手.

其次,我要说一说两位有名气的数学家,他们早年表露出相仿的天资.头一个是**安德雷·玛利·安培**(André Marie Ampère),1775—1836,他才是四岁上下的孩子的时候就习于做长长的心算,那是他从玩摆小圆石子学来的规则去做的.他虽一直擅长于
[364] 心算,并且对于数字生来就有非凡的记忆力,但并不专门修练这种计算能力.**卡尔·弗里德里希·高斯**(Carl Friedrich Gauss),1777—1855,则不然,他在大规模计算上一生花了很多时间.虽然那些计算部分地凭借着他在数论上的渊博知识①,但他早年已显露出了其天资.三岁时候就曾因纠正了他父亲在某些加班费计算中的错误而使之吃惊.无论如何,这也许可以说是他那出类拔萃的智慧自幼就开始发展了的佐证.

另一个不平凡的例子是**理查德·惠特利**(Richard Whately),1787—1863,后来做了都柏林的大主教.五六岁左右时他就显露出了心算方面有相当高的技能.大约三年之后又失去了它.他说:"我很快就开始做很困难的加法,从来都是心算,因为我对数字除计数之外别无所知,也不知道我所用的各种方法叫做什么.不过我相信我那时的算术题主要是关于乘法、除法、和比例的问题…….我做那些题比任何人在纸上做的都快,而且从不记得发

① 关于高斯的技巧的论述,可参看 P. Maennchen, Nachrichten der Königlichen Gessellschaft der Wissenschaft zu Göttingen, 1918 (Beiheft 7), pp.1—47.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

生过什么错误,一天到晚我都从事于计算或幻想.上小学以后,那种热情磨灭了,我在算算术上很迟钝,此后一直如此."虽然他这样说,大主教后来的算术水平比他这里说的好得多.

泽拉·科尔伯恩(Zerah Colburn)1812年在伦敦的表演更为惊人.科尔伯恩1804年出生于美国佛蒙特(Vermont)州卡伯特(Cabot)市一个小农家庭.在未满六岁的时候他就显露出了非凡的心算本领,在美国巡回表演.两年后被带到英国,在那里一再接受权威方面的考验.他能够立即答出两个四位数字的乘积,如果两个数都超过一万,则稍需迟疑.在那时给他提的问题中有"8 [365]
的16次方是多少?"几秒钟内他答出:281 474 976 710 606.这是正确的.然后又要他算出2,3,4,…,9的10次方.他回答得那么快,以致于作记录的先生不得不请他慢点重复一遍.但是当问他两位数(如37或59)的高次方时,回答的速度要稍慢一些.他能立即说出大数的平方根或立方根(当它们是整数时),例如106 929的平方根和268 336 125的立方根.不过,这类整数根很容易用各种方法求得.更惊人的是他对因子分解问题的回答.问以247 483,立答941与263;问以171 395,立答941与263;问以171 395,立答5,7,59与83;问以36 083,回答没有.不过,问以大于1 000 000的数,他就感到困难了.他对大数分解因子的能力特别强,主要依靠后述的双末位数法.和一切这些公演者一样,他必须对付取笑者的戏弄,不过在一般情况下他都能够应付他们.有一次有人问他几个黑豆才能作成三个白豆,据说他立即回答:"三个,你把它们的皮剥掉就是了".但这看起来很像是一场预先安排的表演.

观看的人可以明显的看出这个孩子是按一定的法则运算的,因为在他计算时他的嘴唇在不停地动,好像在用语言表达其过程.这是无疑的.在少数情况下他能够解释他的算法.问他4 395的平方是多少? 他迟疑一下,当你把问题重述了一遍时,他就回答出正确的答案——19 316 025.问他迟疑的原因,他说

我们必须知道,而且我们必将知道

http://maths352.bokee.com

他不喜欢四位数乘四位数，但是他又说："我用别的方法求到它，我用 293 乘 293，再用 15 乘两次."另一次问他 21 734 乘 543，他
[366] 立即回答 11 801 562；问他怎样算的，他说是他用 181 乘 65 202 而得到这个结果. 这些谈话说明一有方便他就把所要算的数先分解因子.

1814 年他被带到巴黎，在当时的政治动乱气氛中他的表演未受到赏识. 但是，他的英美朋友们为他集资受教育，他被先后送到巴黎的吕西·拿破仑(Lycée Napoleon)那里和伦敦的威斯敏斯特(Westminster)学校. 在受教育的过程中他的心算才能降低了，也失去了孩提时代逗人的天真. 他后来的行业屡更且不甚成功. 先尝试于剧坛，继任教员，再在美国做巡回传教士，最后任语言"教授". 他写了自传，其中有他自己用过的方法，1840 年去世.

与科尔伯恩同时代的还有一个自学的孩子，**乔治·帕克·比德**(George Parker Bidder)，他也具有颇为特殊的此类能力. 也许可以说他是这些神童中最有趣的一个，因为他后来受过高等普通教育，保持住了他的计算能力，并在晚年对他发明并使用过的方法作出了分析和解说.

比德 1806 年生于德文郡(Devonshire)亨普斯特德(Hempstead)的摩顿(Moreton)市，父亲是一个石匠. 六岁时学会数到 100，虽然被送入乡村小学，但学的东西甚少，在他发展起步之时，对数学名词和符号一无所知. 仅仅具备了这点数数的知识，他自学了加法、减法和数(小于 100)的乘法，是利用摆石子、钮扣或子弹而练出来的. 晚年他非常重视此类实物表示法，并且深信在他对数学符号毫无所知的幼年正是用实物表
[367] 示加强了他的算术计算能力. 七岁时他听到两个邻人为买卖一件东西的价钱而争吵时，他上去指出了双方都错了，并且说出了正确的价钱. 那次显露之后，邻人们都喜欢给他提算术问题了.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

他的声誉日增.未满九岁时,其父觉有利可图而带他去各地表演.剑桥大学的几个优秀毕业生[托马斯·杰夫森(Thomas Jephson),他后来是圣约翰大学的指导教师,还有约翰·赫谢尔(John Herschel)]在1817年见到他,对其各方面智力的印象极为深刻,故而为他筹集了受教育的资金,并劝导其父放弃其展示生意.但几个月后老比德后悔不该放弃那么容易的生财之道,坚持要他的儿子回去,再度携子到处展示.1818年在其旅途中,小比德与科尔伯恩相遇斗智,总成绩上小比德取胜.最后,父子来到爱丁堡(Edingburgh),那里的大学里几个人出面说服其父将少年留下由他们照管教育.比德就留在那里,届期毕业于爱丁堡大学,不久后就从事土木工程之业,颇享盛名.卒于1878.

随着实践,比德的心算能力不断地发展.他的早期表演似亦不外乎上述巴克斯顿和科尔伯恩的那些类型.除了回答数的乘积和将给定的量化至指定的单位外,1819年后能求大数的平方根、立方根,等等,当然要这些根是整数的情况.后来他解释了所用的方法.他的方法很便于应用,并且和科尔伯恩不谋而合.这时他还能立即答出关于复利和年金的较容易的问题的答案.这对于他的同代人来说要算是在他的一切技能中最令人惊佩的了.在因子分解方面他稍逊于科尔伯恩,一般说来,当数目大于10 000时他不能一望即知其因子分解式.和科尔伯恩一样,也常受到戏弄,但能从容应付.1818年在伦敦的一次表演中,有人问 [368]
他要多少根公牛尾巴接起来才能从地球达到月亮,他应声而答:"一根,只要是足够长的一根."

下边是1815—1819年间在表演时提给他的问题和他给的答案,它们是包括数百个此类问题的可靠资料中摘来的,绝少有实质上困难者.他计算的速度是惊人的,不过所用的时间都是非熟练的围观者记录下来的,只能看成是大致可信的.当然,所有的计算都是心算而绝不借助于本子、笔或纸.1815年,那时他刚

我们必须知道，而且我们必将知道



九岁，问他：假定月亮和地球之间的距离是 123 256 英里，声音传播的速度是每分钟 4 英里，问月亮上的居民在多长时间后才能听到滑铁卢战役的炮声？答：21 天 9 小时 34 分钟，心算时间不到一分钟．1816 年，十岁，刚学写字，但还不会写示大数，他回答了如下的问题：本金为 11 111 镑、年利率为百分之 5，11 111 天的利息是多少？答：16 911 镑 11 先令．一分钟答出．如果 30 个苹果可以榨出一夸脱①的苹果汁，问一百万个苹果可以榨出多少豪格海②苹果汁？答：132 豪格海，17 加仑，1 夸脱，还剩下 10 个苹果．35 秒钟答出．如果车轮周长是 5 英尺 10 英寸，问车走 800 000 000 英里时轮子转多少圈？答：724 114 285 704 转，另余 20 英寸．50 秒答出．问 119 550 669 121 的平方根是多少？答：345 761．30 秒答出．1817 年，十一岁时问他：若蓄水库的容积为一立方英里，河水每分钟流入 120 加仑，多长时间才能充满它？两分钟答出．威廉·赫谢尔（William Hershel）爵士问他：假定光从太阳传到地球的时间是 8 分钟，太阳和地球的距离是 98 000 000英里．如果光从离地球最近的一个星球传到地球需时 6 年 4 个月．问这星球离地球的距离是多远？一年按 365 天零 6
[369] 小时计，一月按 28 天计．答：40 633 740 000 000 英里．1818 年在一次表演时间他：如果某个钟的摆每秒钟摆过 $9\frac{3}{4}$ 英寸，那么 7 年 14 天 2 小时 1 分钟 56 秒内共摆过多远？一年按 365 天 5 小时 48 分 55 秒计．答：$2\,165\,625\,744\frac{3}{4}$ 英寸．不到一分钟答出．如

---

① 夸脱（quart），英液量单位名．1 夸脱 $= \frac{1}{4}$ 加仑 $= 1.1375$ 公升．——译者注

② 豪格海（hogshead），英液量单位名．1 豪格海 $= 52\frac{1}{2}$ 加仑．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com

果我有 42 只表要卖，第一只卖价一法寻①，第二只价钱是第一只的两倍，第三只的价钱又是第二只的两倍，依此类推．问最后一只表的价钱是多少？答：2 290 649 224 镑 10 先令 8 便士．如果一个便士的直径是 $1\frac{3}{8}$ 英寸．用一个挨一个的便士把世界围一圈．它们的价值一共合多少英币？假定一圈分为 360 度，每度跨 69.5 英里．答：4 803 340 镑．一分钟答出．求两个数，它们相差 12，而它们的积与和相乘等于 14 560．答：14 与 26．求一个数，它的立方减 19 再乘以它的立方等于 6 的立方．立即答出：3．要修一条 21 英里 5 浪② 37 杆 4 码长的马路，每英里费用为 123 镑 14 先令 6 便士．问总的费用是多少？答：2 688 镑 13 先令 $9\frac{3}{4}$ 便士、两分钟答出．如果你现在是 14 岁，并且要再活 50 年，每天花半克朗③．问你今后要花多少法寻？答：2 805 120．15 秒钟答出．穆尔先生承包以 22 965 321 盏灯照明伦敦市．每盏灯的安装与点燃费用是 7 法寻，每三盏灯耗油 $\frac{2}{9}$ 品脱④，油价是每加仑 3 先令 $7\frac{1}{2}$ 便士；他的收益是投资的百分之 $16\frac{1}{2}$．问共耗油多少？投资多少？承包金额是多少？答：用油 212 641 加仑，投资 205 996镑 16 先令 $1\frac{3}{4}$ 便士，承包金额是 239 986 镑 13 先令 2 便士．

---

① 1 法寻(farthing) = $\frac{1}{4}$ 便士 = $\frac{1}{960}$ 镑．——译者注

② 浪(furlong)，英制长度单位．1 浪 = $\frac{1}{4}$ 英里 = 220 码 = 44 杆．——译者注

③ 克朗(crown)，英币名．1 克朗 = $\frac{1}{4}$ 镑 = 5 先令．——译者注

④ 品脱(pint)，英液量单位．1 品脱 = $\frac{1}{8}$ 加仑．——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



应当注意，比德看待一个数不是从字码的形象去认识它而是心目中予以具体的形象．例如把984想成是那么多的单位，可以把它分成24组，每组21个．还要注意，他和后边我要说的伊瑙迪
[370] (Inaudi)一样，主要是依靠听觉而记住数字．“就我自己来说”，他晚年写道，“虽然也很习惯于阅读以常用符号表示的数量，如果要把写在纸上的数字记住，那将比记住听来的数字需用长得多的时间和大得多的努力．”例如，假定问题是求两个九位数的乘积，如果把它们“读给我，我不会要求读第二遍；但是如果写到纸上再递到我手里，我将可能要花四倍的时间去仔细阅读才能记住它们，而且即使那样，脑子里的印象也不怎么深刻而生动．”

比德终生都保持着迅速心算的能力，而且做有涉工程事项的常任议会见证人工作是很出色的．临去世前还在他的一位朋友面前显示了他的特长．友人在谈到那时的新近发现时提出：如果一英寸内要有36 918个波长的红光才能给人以红色的感觉，光速为每秒钟190 000英里，那么一秒钟内有多少个光波射入人眼使感觉出红色呢？比德接着说：“你不必算了，这个数字是444 433 651 200 000．”

比德家族的其他成员也都有类似的特异功能和非凡的记忆力．比德的兄长之中有一位任保险公司的计算员．在一场火灾中他的帐本都被烧掉了．他根据记忆花六个月的功夫把它们都背写了出来，据说随后就死于脑膜炎了．比德的另一位普里穆斯教友派兄长能背诵全部圣经，并且能说出任一经句在哪一章第几节里．比德的长子是一位卓越的律师，能心算两个十五位数的乘积，不过无论在准确性上或速度上都不能与其父相比，但是他也从未坚持发展自己在这方面的才能．他说他在心算时是用数字
[371] 的形象进行的：“我在做加法时心目中总是有一个可见的形象；实际上我也没有别的心算办法．”我们注意他这是和其父不同的．他的孩子中一子一女，也就是比德的一个孙子和一个孙女，也有类似的天赋．

我们必须知道，而且我们必将知道

其次提到亨利·蒙窦(Henri Mondeux)与维多·曼伽美尔(Vito Mangiamele). 两人皆于 1826 年出生于贫寒之家,俱为牧人,自幼皆以心算见长而名传乡里. 二人分别于 1839 年和 1840 年被带到巴黎演示,受到阿拉戈(Arago)、柯西(Cauchy)等人的考验. 蒙窦的演示更为惊人. 有一个提给他的问题是解方程 $x^3+84=37x$,对于这个问题他立即答出一个根是 3,另一个根是 4,但没有察出第三个根—— -7. 另一个问题是求不定方程 $x^2-y^2=133$ 的解组. 他立即回答出一组解是 66 和 67. 要他找一组较简单的解,稍过一会儿他说出 6 和 13. 不过,我不想多谈他们的才能,因为对他们的朴实性是有怀疑的,那些利用他们的人教给了他们些窍门,使得他们能装出一些似有而实无的才能. 最后两人都回去务农而对科学的世界不再感兴趣. 如果蒙窦是自学来的,那么我们应当把某些代数定理的发明记给他一份功绩,但是那样的话又使人不可理解为什么他从未做出任何稍多的贡献而他的才能似乎总是局限于他所解答的那些个别的问题.

我下一个要说的是约翰·马丁·查恰理亚斯·达泽(Johann Martin Zacharias Dase),他是这些心算神童中有趣得多的一个例子. 达泽 1824 年生于汉堡. 他受过良好的教育,发展才能的每种机会都提供给他了,但是除了与计算及数字有联系的方面稍有进步外,观察他的人所得印象像是个傻子. 他对于几何学和除德语外的任何语言至死一窍不通. 他是诚实的,在德国的许多下级 [372]
机关里补过职. 他在德国、澳大利亚和英国都展示过他的心算才能,死于 1861 年.

1840 年他在维也纳表演的时候结识了斯特拉斯尼斯基(Strasznicky),斯氏敦促他把他的才能灌注于科学事业. 达泽欣然接受劝告,于是认识了高斯、舒马赫(H.C. Schumacher)、彼德森(A.C. Peterson)与恩克(J.F. Encke). 后边我要提到他在科学上的贡献. 在心算方面我唯一能查到的简易问题是:舒马赫问 79 532 853 乘 93 758 479 是多少,54 秒钟作出回答. 在回答两个

我们必须知道，而且我们必将知道

http://maths352.bokee.com

二十位数相乘的问题时，他用了 6 分钟，在回答两个四十位数相乘的问题时，他用了 40 分钟；在回答两个一百位数相乘的问题时，他用了 8 小时 45 分钟．高斯估计一个熟练的计算者在纸上演算最后这种问题时用一半的时间就够了．达泽有一次在 52 分钟里心算出了一个百位数的平方根．这些成绩远远超过了同类的其他记录，仅可比美的是巴克斯顿的心算 39 位数的平方与瓦里士的开一个 53 位数的平方．不过，达泽的心算不总是正确的，有一次（1845 年），提给他的每个问题他算的结果都不对，但那时他正生病头疼，失败不足为怪．

和所有这些心算神童一样，他也有惊人的记忆力，表演过后一两个小时他仍能重述所有的数字．他还有一种奇才——一望即知羊群里有几只羊、书架上有几本书（数目不超过 30 时），等等；还能回想大量物体的形状和数目．例如在一些骨牌上看一秒钟之后就能说出它们的点数总和（117）；在一张大开的印刷品上随便指给他一行看一眼后问他有多少字，他立即答出正确的数
[373] 目（63）；写十二个数码，让他看半秒钟，他就能记住它们和它们的位置，从而能说出哪个位置上是哪个数码．可惜我们不知道更多的此类表演．熟悉罗伯特乌丹（J．E． Robert-Houdin）的有趣的自传的人都会记得他是怎样培养类似的能力的，并且他在技能锻练中感到它多么可贵．

当允许使用纸和笔时，达泽的计算快得令人难以置信而且从来都准确无误．十六岁时斯特拉斯尼斯基教给他众知的公式 $\pi/4=\tan^{-1}\left(\frac{1}{2}\right)+\tan^{-1}\left(\frac{1}{5}\right)+\tan^{-1}\left(\frac{1}{8}\right)$ 的应用，并要他利用它去计算 π．两个月后他把近似值计算到小数点后二百零五位，前二百位是正确的[①]．达泽的下一项功绩是计算前 1 005 000 个

① 此结果公布于 Crelle's Jouranal，1844，Vol．XXVII，p．198；关于更精确的近似值和较容易的公式，参看本书第 12 章．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

数的自然对数,算到小数点后七位.这项工作是1844到1847年间担任普鲁士的测量期间在工作中休息时做的.其后的两年间他在闲暇时编制了一个双曲线函数表,1857年由奥地利政府出版.后来他提出要编制从7 000 000到10 000 000的所有整数的因子表.由于高斯的推荐,汉堡科学院同意帮助他好让他从容不迫地去干,但是大约只干完了一半他就去世了.

特鲁曼·亨利·萨福德(Truman Henry Safford)是又一个心算神童,1836年出生于美国佛蒙特(Vermont)州罗亚尔顿(Royalton)市.他的情况有些不同,受过良好的教育,届时毕业于哈佛大学,最终从事于天文学,并在该科目上取得教授职位.我查得他虽然一向算得很快,但逐渐失去了年轻时的特殊能力,死于1901年.

萨福德从不当众演示他的心算才能,我是从斯克里普丘(Sripture)和米切尔所引的报导里才知道的,但那些似乎是这些计算者的典型.1842年,他的心算使家里的人吃惊而且高兴. [374]
1846年,那时他十岁,受到了考验.下边是几个提给他的问题.求某个七位数的立方根,立刻答出.一个数被它的各位数码的乘积除时商是3,并且加上18后它的各位数码的次序恰好颠倒,问此数为何?答:24.大约用了一分钟.一个正棱锥的斜高是17英尺,底是边长为33.5英尺的正五边形,问此锥的表面积是多少?答:3 354.555 8平方英尺.两分钟答出.问某个十八位数的平方是多少,大约在不足一分钟的时间里答出,但是如果这数是由数码365重复六遍而构成的,问题就更容易些.和科尔伯恩一样,他也能轻而易举地将大数分解因子.在这些事例中他所用的是经验法,即,他选取(他也说不出怎样选法)可能的因子并在不多几秒钟里实行试除而检定之.

新近有四位心算者颇有名气:**乌戈·札姆博恩**(Ugo Zamebone),意大利人,生于1867年;**帕瑞克尔·迪亚曼狄**(Pericles Diamandi),希腊人,生于1868年;**卡尔·吕克勒**(Carl Rückle),德

我们必须知道，而且我们必将知道

http://maths352.bokee.com

国人;雅克·伊瑙迪(Jacques Inaudi),生于1867年.前三位属通常的类型,我不打算记述他们的事迹了,但伊瑙迪的事迹值得详述.

伊瑙迪①1867年出生于意大利的奥诺拉托(Onorato).幼年为他人牧羊,过了长时间的优闲日子,无须和数字打交道,但也不使用小石子之类的实物去表示数目.大约1873年左右,他的心算能力开始受到注意.不久之后,其兄去普洛旺斯(Provence)摇筒风琴谋生.小伊瑙迪跟着去见了世面,也借街头表演给自己赚了一些小钱.杂技团长雇用了他,1880年去巴黎演出.那里所
[375] 有的观众对他的印象都是既谦恭、坦率而又诚恳.他那时尚不知读书写字为何事,那是后来才学习的.

他早期的表演并不像别的心算神童那么特别惊人,但随着实践他不断地进步.1873年在里昂时他能几乎立即答出两个三位数的乘积.1874年他能回答两个六位数的乘积.九年之后他能用九位或十位数迅速进行计算.稍后在巴黎时达布(G. Darboux)问他27的立方,他十秒钟答出.在十三秒钟内他算出了18年7个月21天3小时内有多少秒钟;又几乎立即答出4 801的平方与1的差的六分之一的平方根.他还轻而易举地计算出传说的故事中应当付给塞萨(Sessa)的小麦的数量,他因发明象棋而得到棋盘上第一个方格中的1喱小麦、第二个方格中的2喱小麦、第三个方格中的4喱小麦,照此依等比级数类推.

他能求方程的整数根和问题的整数解,但只是用试差法.他最惊人的技艺是将小于10^5的数表达为四个数的平方和,一般要用一两分钟.这种能力是他特有的.此类问题都是在非公开的表演中解答的,那时他的脑力也极为劳累.

---

① 参看 Charcot and Darboux, Mémoires de l'institut, Comptes Rendus, 1892, Vol. CXIV, pp.275, 528, 578;以及 Binet, Révue des deux Mondes, 1892, Vol. CXI, pp.905—924.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

每次公开表演很少有超过 12 分钟的,所以是比较简单的事.一个正常的节目单包括从一个二十一位数里减去另一个二十一位数,五个六位数相加,两个四位数相乘,一个九位数开立方,一个十二位数开五次方,问到几年几月几日有多少秒,某年月日某日是星期几.当然,这些问题都由听众提.对于一个职业计算者说,这些都不是特别困难的问题.当每个问题中的数字被 [376]
宣告后,伊瑙迪把它慢慢复述给他的助手,助手把它写到黑板上,然后大声念一遍以确认无误.然后伊瑙迪再念一遍.一般地这时答案已经算出了.如果他需要较长的时间,他就说几句一般性的话,这不妨碍他在同时进行心算.在整个表演过程中他都面向听众,从不再向黑板上看,这样使得表演的效果更好.

记忆数字的不同方式

可能大多数心算神童都是依靠语言肌、眼和耳去记忆那些要算的数字.先前认为他们都摹想提给他们的数字,有些人确实是那样做的.然而伊瑙迪却主要是靠耳朵去听那些音节.比德也部分地靠耳听,当他摹想一个数的时候,眼前浮现的不是一串数码而是一团具体的单元,如果数目是一个合数,这些单元就分成许多确定的小组.吕克勒则主要依靠摹想.可见心算者们的记忆方式是不同的.伊瑙迪能够在心中再现他自己复述数码的声音,如果把数字写给他看,那对他不但无用而且是帮了倒忙.数字的每个数码的音节似乎对他充分发挥才能是必要的.他习惯于在开始心算之前先大声朗读数据——声音串才是重要的.当读给他一个二十四位数时,59 秒钟内他就记住了它的声音,于是他就能背诵或倒背这串数码,而且不论从哪一位开始都行.这么做蒙窦需要 5 分钟后才行.大致百位数字的相仿的记忆对于伊瑙迪需 12 分钟,迪亚曼狄需 25 分钟,吕克勒需要近 5 分钟.这种能力只限于数字,计算者们一般都不能记住一长串文字.伊瑙迪脑子里一天到晚想的都是数字,很少想别的什么.他梦到的也是数字,有时候甚至在睡梦中解算问题.他对数字的记忆力是卓绝 [377]

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的，但对其他事物的记忆力则和一般人一样，有时甚至不如.表演结束后他还能背出给他提的那些问题和他的答案，包括总起来几百个数码.他对这种事情的记忆并非限于几个钟头之内.有一次给他提了一个包含二十二位数的问题，八天之后，突然又问他那个问题，他立刻说出了那个数字.他受过多次测验，我们对他的情况所知较对他以前诸人(可能除比德以外)所知较多.

比德所用方式的分析

这些心算神童中大多数人觉得要他们解释他们的算法是困难的甚或是不可能的.不过我们有当时有学识的观众对他们的计算过程的一点分析.

值得注意的一则是比德谈他自己的算法，另一则是科尔伯恩谈他自己的算法，其他还有缪勒(Müller, G.E.)谈吕克勒的算法和达布谈伊瑙迪的算法.比德所谈最为完整，他人所谈大体相近.

比德的关于他发明并使用的方法的说明包括在 1856 年他在土木工程学会上所作的报告里[1].在叙述这些方法之前，有两点一般性的注意事项，我想在读他的报告书时是应当记在心中的.首先，他以其完善的形式给出他用的方法，而未必是他在孩提时代所用的形式；此外，他在实践中可能用了什么装备简化工作，不过他在报告中没有摆出来.其次，他和别的神童们都有优异的记忆力，并且在不断的实践中又继续提高了，虽然他认为不是这样，但这是可以肯定的.一个例子就足以证实这个看法.1816 年在一次表演中，把一个数倒念给他，他立即把它正念出来.一小时后问他是否还记得它，他立即背了出来，一字不错.那
[378] 数是：2 563 721 987 653 461 598 746 231 905 607 541 128 975 231.

---

① Institution of Civil Engineering, Proceedings, London, 1856, Vol. XV, pp.251—280.报告的一份初稿尚存于数学会.其中的多样性很有趣，表明了他的记忆力发展的进程，但无必要在此作详细的引证.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

四个基本运算中,加法和减法没有什么困难也没趣味.唯一似乎值得注意的一点是比德在加三个或更多个数时总是一个一个往上加,如下边的例子所示.他认为迅速的心算依靠合理的安排,凡有可能时都要安排得使每次只做一件事.这在伊瑙迪的计算中也是可看出的.

比德最先碰到的自然是一个数被另一个数乘.他六岁时自学了直到 10 乘 10 的乘法表.不久他就练习较难的算术问题,因为是乡村铁匠的一个宠儿,经常在铁匠铺子里,人们就习以为常围坐于炉火旁问他些乘法问题.从两位数相乘开始,回答那些问题时他用不着人们可以觉察到的停顿时间去思考,然后提高到三位数相乘和四位数相乘.他的努力得到半便士的报酬.到了八岁时他能心里将两个六位数相乘.有一次他甚至做了两个十二位数的相乘,不过他说"这要很多时间"并且"是艰巨而苦恼的事."

原理上,他所用的方法和通常的教科书上所讲的相同,不同的是他在进行中一路加出他的结果.例如用 173 乘 397 时,他是如下进行的:

先算	$100 \times 397 = 39\,700$
在此结果上加	$70 \times 300 = 21\,000$ 得 $60\,700$,
在此结果上再加	$70 \times 90 = 6\,300$ 得 $67\,000$,
在此结果上再加	$70 \times 7 = 490$ 得 $67\,490$,
在此结果上再加	$3 \times 300 = 900$ 得 $68\,390$,
在此结果上再加	$3 \times 90 = 270$ 得 $68\,660$,
在此结果上再加	$3 \times 7 = 21$ 得 $68\,681$. [379]

如果假定每步用一秒,这将低估了他的速度,但即使按这个低于实际的速度推算,他也会在 7 秒钟内给出答数.按这个方法,他永不拿多于两个的数相加,并且每步中的乘数都只有一个非零的数码.这是心算者们常用的算法.在此还要指出,比德总是从左到右进行,虽然通常小学里不是这样教,这是自然而又方

我们必须知道，而且我们必将知道

http://maths352.bokee.com

便的算法.事实上,他把(100+70+3)与(300+90+7)或$(a+b+c)$与$(d+e+f)$的乘积安排成$ad+ae+\cdots+cf$.

像上边所给的乘法,其结果似乎是转瞬即得,这使他实际工作中能利用直到1 000乘1 000的乘法表.在这个基础上,当他计算很大的数的乘积时,例如965 446 371乘843 409 133时,他把大数截成每三位一段,相乘时好像965与446等等各是一个数码,不过以1 000为基数而已.中年时代他算此类问题大约用6分钟.在计算这些乘积时他的困难与其说在于乘法本身不如说是在于回忆前一步的结果.

伊瑙迪也是这样乘的,但他只要求乘时因子之一只有一个非零数码.有时他也利用负数.例如,他把27×729想成$27\times(730-1)$;还有,把25×841想成84 100/4.在求数的平方时,他习惯于把一个数想成$a+b$的形式,并且把a与b选取成适当的形状,然后计算$a^2+2ab+b^2$而得到结果.

在用一个数乘具体的数据时,比德的做法和上边所说两个数相乘的步骤相同.例如用787乘14镑15先令$6\frac{3}{4}$便士,他是这样做的:

先算(787)(14)镑=11018镑0先令0便士,

加上(787)(15)先令=590镑5先令0便士,

得　11 608镑5先令0便士,

再加(787)(27)法寻=22镑2先令$8\frac{1}{4}$便士,

[380] 得　11 630镑7先令$8\frac{1}{4}$便士.

比德的除法更像小学课本上的做法,不同的是他那一望即知大数乘积的能力使他能够巧猜而省掉不必要的工作.伊瑙迪也是这样.带余数的除法要比较困难.比德对付这种问题比这些神童中大多数都更熟练些,但即使在他的盛年之时他也从未像解决无余数的除法问题那么快地解决有余数的除法问题.在公

我们必须知道，而且我们必将知道

http://maths352.bokee.com

演中,通常规定不许提麻烦的除法问题.

如果比德知道一个除法问题里没有余数,他常常就用双末位数法.举例来说,若要用 176 除 25 696.他先判明答案是一个三位数,而且显然最左边的一位是必是 1.然后他注意到只有 4 个二位数(即 21,46,71,96),它们之中任一个与 76 的乘积的末两位是 96.所以答案必是 121,146,171 或 196.经验能使他不用计算就断定 121 太小而 171 太大.所以答案必是 146.如果他觉得有点迟疑,那么心算一下 146 与 176 的乘积(他说他能够“立即”做到)去验证结果.值得注意的是当比德、科尔伯恩还有一些其他计算神童都知道两个数的乘积的末两位数码.他们还也许潜意识中知道各个数的末两位必定具有某些形状.米切尔曾讨论过这双位数码配合的理论.

在做除法时,比德常常用我把它叫做“和码法”的一种方法,这方法初看来比常规的方法麻烦得多,可是在他手中这个方法却特别迅速,所以我想这是个特别适合于他的方法.我把“和码”定义为:求原数各位数码的和的各位数码的和的……,直到得的和小于 10 为止,此个位数即是原数的和码.一个数的和码与它的各个因子的和码的积的和码是相同的.让我们照比德的做法 [381]
把这个论断用于检査 71 是否 23 141 的一个因子.23 141 的和码是 2.71 的和码是 8.如果 71 是一个因子,那么另一个因子的和码必须是 7,因为只有 7 与 8 的乘积的和码才是 2.另一方面与 71 的乘积的末两位数是 41 的数只有 71.又因为另一个因子必是三位数且其和码必须是 7,所以这个因子(如果有的话)必须是 871.但是粗略地一看就知道 871 太大了,所以 71 不是 23141 的因子.比德认为这个方法比直接用 71 试除要快得多.作为另一个例子,让我们再来看看 73 是不是 23 141 的因子.23 141的和码是 2;73 的和码是 1,所以另一个因子(如果有的话)的和码必须是 2.但是因为末两位数是 41,这另一个因子(如果有的话)必须是 17.又因为这个因子必是三位数且其和码为 2,这样的因

我们必须知道，而且我们必将知道

http://maths352.bokee.com

子如果存在话,必是 317. 检验(用 73 乘它)后知道它确实是一个因子.

当他开始公开表演时,当然啰,人们经常向他提出一些关于重量和大小的问题. 在解答这些问题的过程中,他记住了问题中经常出现的许多关系,像一年是多少秒,一吨是多少两、一亩是多少方寸、一百镑是多少便士,以及民历与基督教会历的基本规律等等. 一大批此类数字是所有心算神童们的一部分装备.

比德在他表演时常常遇到求平方根或立方根的问题,后期还有开更高次方的问题. 他的随口即答使那些慕名而来的听众惊叹不已. 不过,如果答案是整数,那么这只是任何人都能练得出来的技艺. 不必详述其规则,几个例子就可以说明他的方法.

要他求 337 561 的平方根. 显然这个根是一个三位数. 由于所给的数在 500^2 即 250 000 与 600^2 即 360 000 之间,这个根的
[382] 最左边的一位数必是 5. 他想到平方后末两位是 61 的二位数只有 19,31,69,81,这他是很熟悉的. 所以答案是 519 或 531 或 569 或 581. 他继而论证因 581 与 500 和 600 的比差不多和 337 561与 250 000 和 360 000 的比相同,故答案必是 581,他再花两秒钟用乘法直接验证一下这个结论. 相仿地,在求 442 225 的平方根时,他立即看出答数的最左边的一位数码是 6,又因为原数的末尾是 225,所以答数的后两位是 15,35,65 或者 85. 442 225在$(600)^2$ 与$(700)^2$ 之间所处的位置指明应当取 65,故答数是 665. 验证之后他才宣布它. 其他心算者曾订出类似的开平方规则.

对于开立方,这个方法更快. 例如,要求 188 132 517 的立方根,比德一望即知答数是三位数且因 $5^3 = 125$ 和 $6^3 = 216$ 故答数最左边的一位数码是 5. 两位数中,立方的末尾是 17 者只有 73. 所以答数是 573. 相仿地,180 362 125 的立方根也是三位数,它的最左边的一位也是 5,右边的两位可能是 65 或 85. 为了弄清

我们必须知道，而且我们必将知道

http://maths352.bokee.com

应该是哪一个，他心中算一下560的立方.看到它和所给的数很接近，就初步断定所要的答案是565，然后再用乘法验证一下.一般地，用这个方法去看清一个末位数码为5的立方根要比看清一个末位数码不是5的立方根稍微难一点.不过因为这时5^3必为原数的一个因子，所以可先用5^3除原数，再用上述方法求商数的立方根.譬如，上边那个数180 362 125等于$5^3 \times$ 1 442 897，由此马上求得立方根是5×113，即，565.

对于求更高次的精确方根，这方法更简便.特别是求五次方根几乎容易到乏味了，因为原数的末位数码永远和它的五次方根的末位数码相同.于是，当提出的数小于10^{10}时，答数是一个二位数.只要记住10，20，…，90的五次方都是些什么数，我们为要断定答数的第一个数码只须看清所提的数在它们之中哪两个 [383]
之间，答数的末位数码是明显的，所以可立即给出答数；如果提的数更大些，但小于10^{15}，答数是一个三位数，中间的数码也几乎和其他两位数码一样快地找到.这与其说是心算还不如说是一个巧技.

在后来的表演中，有时候要比德求的方根可能不是整数，但要求把整数部分求出来.如果他觉察到所求的根会是非整数，就用“弃九法”去检验它，如果确信答数不是整数，他就尽力去试着求.当答数有三位或四位整数时，此类问题对于一个心算者是很吃力的，常常在公开表演时予以禁止.

科尔伯恩的在数的分解因子方面的惊人技能也表现在提给比德的相仿问题上，他逐渐也研究出一些法则，但在心算这类问题上我不认为他曾达到精通.当然，如果因子是2或5的乘幂，他能立即得到；如果因子是3的乘幂也可以几乎一样快地得到.对于接近于某个数的平方根的因子，他总是试用通常把一个数表示成为a^2-b^2的形状，这样一来，因子是很显的了.对于其他的因子，他试用上边说的和码法.

比德对于复利和年金的问题能够几乎立即给出答数，这是

我们必须知道，而且我们必将知道



他的擅长，而且他的方法是很简单的. 可以用一个例子说明他的方法. 设要求本金为 100 镑、利率为百分之五，14 年的复利. 他分析：单利是(14 镑) × 5，即 70 镑. 一年之后本金增加 5 镑，它的单利是每年 5 先令，即一克朗，这一项持续 13 年. 第二年后，本金又增加 5 镑，它又以每年 5 先令的单利持续 12 年. 继续这个分析，利息的总数是(13 + 12 + ⋯ + 1)克朗，即(13/2)(14)(5)先令，或 22 镑 15 先令 0 便士. 它与单利 70 镑相加共为 92 镑 15
[384] 先令 0 便士. 然后，第二年终所得的 5 先令(它是第一年终所得 5 镑利息的利息)以后每年又得利息 3 便士，此项利息持续 13 年，共计(12/3)(13/2)(14)(3)便士，即 4 镑 11 先令 0 便士. 它与前两项利息的和 92 镑 15 先令 0 便士相加是 97 镑 6 先令 0 便士. 相仿地，在此数目上还应加(11/4). (12/3)(13/2)(14)(3/20)便士，即 12 先令 6 便士，总数为 97 镑 18 先令 6 便士. 在此总数上再加(10/5)(11/4)(12/3)(13/2)(14)(3/400)便士，即 1 先令 3 便士，总数增至 97 镑 19 先令 9 便士. 在此总数上再加(9/6)(10/5)(11/4)(12/3)(13/2)(14)(3/8000)便士，即 1 便士. 总数又增至 97 镑 19 先令 10 便士. 剩下还应加上的利息不足一个法寻，所以他立即回答复利为 97 镑 19 先令 10 便士. 解答这个特例他实际占用的时间不到一分钟——这要比大多数数学家借助于对数表计算所用的时间短得多. 注意在他的分析中他计算了许多级数的和.

按通常的记法，复利的本利和是 $(1.05)^{14} \times 100$ 镑. 若将 100 镑记为 P 并将 0.05 记为 r，则本利和即 $P(1+r)^{14}$ 或 $P(1+14r+91r^2+\cdots)$，当 r 很小时，这个级数收敛得很快. 比德实际上是论证了级数的前相继几项，并当发觉后边的项充分小时就把它们弃掉.

在比德的这个报告中说到如果他记忆结果的能力能有他其他方面的智力那么强的话，他会很容易地计算对数. 几个星期之后，他着手解决这个问题，并且设计出了一个心算七至八位对数

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的方法①.他要一位朋友检验一下他的准确性,相继答出了以下数字的八位对数,这些数字是 71,97,659,877,1 297,8 963,9 973,115 429,175 349,290 011,350 107,229 847,369 353.所用时间分别从三十秒到四分钟不等.这些数都是素数.答案大部分都是对的,个别有点误差,多半是末一位上的误差,而且在一经 [385]
指出后就立即纠正了.这个惊人的表演是比德在年过 50 后进行的.

亚历山大·克莱格·艾特肯(Alexander Craig Aitken)堪称本章人物中的冠军,他不仅是首屈一指的心算神童,而且是第一流的数学家,四本书和七十来篇论文的著作者.他 1895 年生于新西兰的丹尼丁(Dunedin)市,在第一次世界大战中服役直到 1917 年负伤.1923 年离开新西兰去爱丁堡.他的哲学博士论文一鸣惊人而升级授予科学博士学位.嗣后一直留在那里,于 1946 年继爱德蒙·惠特克(Sir Edmund Whittaker)任教授之职.他是一位最能激励人的教师,他的学生们都极爱和他交往.他那非凡的心算能力②部分地是因为他有着罕见的记忆力.他能背诵威吉尔(Virgil)和弥尔顿(Milton)的大段诗篇.有一次他说他不能轻易为消遣而阅读,因为读后很难再把它忘掉.他偶尔也当众表演,在瞬间里做一些乘法、除法、开平方和开立方,并在黑板上(凭记忆)迅速写出尚克斯所算 π 的 707 位近似值(参看本书 363 页).1945 年当弗格森(D.F.Ferguson)告诉他尚克斯的结果在第 528 位上错了时,他毫不费力地回想出了正确到 1 000 位(据米勒

---

① 参看 W.Pole, Institution of Civil Engineering, Proceedings, London, 1890—1891, Vol. CIII, p.250.

② A.C.Aitken, "The Art of Mental Calculation; with Demonstrations," 载于 Thansactions of the Royal Society of Engineers, London, 1954, Vol. XLIV, pp.295—309.并参看 Proceedings of the Edinburgh Mathematical Society, 1968, Vol. XVI (Series Ⅱ), part 2, pp.151—176 上的讣闻.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

说，是 2 000 位)的 π 值.有一次他说这个回想过程是“很有节奏的”.更非寻常可比的一项特技是迅速计算特殊的行列式.

他在比赛中胜过了威姆·克莱茵(Wim Klein)，后者是一个荷兰的心算神童，能记忆直到 100×100 的乘法表，但由于缺乏
[386] 数学知识而不会利用巧妙的捷径.爱特肯常常做下意识的计算.他讲到过一些“来得莫名其妙”的结果，有时说他“觉得”某个数是素数，而果然就是素数.他是很少见的与整数为知己的人中之一.例如，他发现 163 有一个有趣的性质——$e^{\pi\sqrt{163}}$与某个整数之差小于 10^{-12}.正像他本人说的，“熟谙数的性质，受自天赋而又不断砥砺之，则能洞查代数与分析的深邃定理.”

他的朋友们和学生们都亲切地记得他那无比的和蔼与宁静.他不仅有多方面的成就，而且还是一个天才的音乐家.他能拉小提琴和中提琴、谱歌、作钢琴曲，还写过一些交响曲(如他所说，这些都严格地“密而不宣”).

[387] 1965 年因健康欠佳而辞退数学主席的职位，两年后逝世.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

第14章 密码术与密码分析

秘密信息——谁掌握它的密钥谁就能识破它而别的人则不能——其编写技巧的研究已有数百年的历史.这种信息的用处,特别在战时,是很明显的;另一方面,它们的破译对敌方也是非常重要的.和这个课题有关的传奇、想发现秘密的好奇心,以及对一切局外人的才能所提出的挑战把本来对它的用处不关心的人的注意力也都吸引到这个课题上来了.

虽然传递信息的方式有多种,但这里只讨论书写的或其他持久形式的秘密信息.所以,轻微的肌肉运动,例如按莫尔斯(Morse)点画系统作长短呼吸,用扇子或手杖打信号,均不在考虑的范围之内.我们所考虑的信息的主要特点是对于那些可能得到它的副本但却不掌握其密钥的人是保密的.因此我们认为那些表面看来可识而实际上传递着另外的隐秘含意的信息是秘密的①.另一方面,一个用外国语文或像速记符号之类的任何可认识的信息"不"是秘密信息.

著名的塞缪尔·佩皮斯(Samuel Pepys)日记通常都说是用密码写成的,但实际上用的是谢尔顿(J.Shelton)②发明的电码.不 [388]

---

① 关于此类的两个例子,请读者参看 Cryptographie Pratique, A.de Grandpré, Paris, 1905, p.57.

② J.Shelton, Tachy-graphy, 1620年第1版,佩皮斯用的是1641年出的第6版.卡特赖特(W.Cartwight)的一种类似系统在1644年由里奇(J.Rich)以Semographie题名发表于伦敦.

我们必须知道,而且我们必将知道

http://maths352.bokee.com



过，日记确实有点难读，因为元音常常被略掉了，而且佩皮斯还使用一些自造的符号去代表某些字尾、独立成分和常用字．还有，在一些难于适当表达的地方，他就由英文换到它种语文，或插入些不要紧的符号．当首先着重于日记时，谢尔顿的电码就被忘了．因此我们可以说，对于初次试读它的人简直就是密码．但是佩皮斯的同代人宁可把日记根本看成是用速记法写成的，虽然它包含着对他的发明的少量修正．

单是信息被隐蔽起来或者以秘密的方式传送它不能认为它就是秘密信息．关于秘密通信的故事大多数说的都是信息保密的技巧或秘密传送信息的技巧，都未涉及密码术．许多古代的秘密通讯例子都属于这种类型．希罗多塔斯（Herodotus）讲到过一种办法，那是先给一个奴隶剃光了头再把信息涂写在他的头顶上，等到他的头发长长之后再把他派出去送信．近代的例子有用鸽子送信，或者把信写在纸烟的包装纸里，等等．

密码术体系　任何一个将明电码转换成密电码的方法都包含两个部分：(1)一个基础的、不变的体系，称为*通用体系*，(2)一个可变的、通常由一个字、词组或一串数码组成的一个秘诀，称为*特定密钥*．通常假定"*敌方*"（任何一个未经许可而持有密信并企图破译它的人）掌握通用体系的全部知识．（这个假定的依据
[389] 是这样的事实：任何大型的通讯系统都不可能将它的通用程序常久保密，也不可能随意改变其通用程序，因为训练人员掌握新方法的困难是很大的．）所以任一种密码规则的相对安全性被认为是与判定其特定密钥所需时间的长短成正比．有鉴于此，可以认为将特定密钥每天改换一次以上通常是不实际的．因此，如果所有的密电（或者其中的大部分）都被截获，那么敌方有时会有几百条密电可用以判定一个特定密钥．这一点常被忽视．由于当只考虑到仅有一条密电被截获时要想破译是非常困难的，甚至是不可能的，因而许多安全性本来是很低的方法往往在它们的发明者心目中被估计得过高了．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

按照处理原始信息的方法，可将通用体系分为两大类．如果仅只将明电码的字符重新排列而本体不作任何更改——即对原来的字符进行轮换——这种方法称为换位法．但是，如果字符本身被换为等价的字母、数码或任何符号，而不改变原来的顺序，则这种方法称为替代法．这两种方法可以综合到同一个密码编制法里，在用一个方法所得的结果上再用第二个方法加以处理．

在本章将给出的这一课题的简论中，将试图对古典的编制密码的方法作一概略的叙述．在每种情况下都附带说明破译的方法．说到这里，要提醒读者注意“翻译”与“破译”这两个词的含意的差别．前者指的是完全掌握译成密码的方法的真正通信员所遵循的步骤，他只需要把译成密码的步骤反过来就行了．后者指的是敌方应用现在称为密码分析这一学科的原理去暗自获取译文所用的方法． [390]

换位法　实际上每一种换位法都用到一个几何图形，在其中按照一定路线填入明文信息，然后再按照另一条路线转换成密码．

下边是用通常称为路线换位法译成密码的一个例子．假定要传递的信息是

I MUST HAVE ANOTHER HUNDRED DOLLARS

假定说，通用方法要用一个完全填满的八列的长方形格子，那么，如果信息中字母的个数不是 8 的倍数，则须增加伪码．本例中需要两个假码，譬如 XX，把它放在信息的后边，这样一来，共有 32 个字母．其次假定填入的路线是从左上角起横行向右，到右上角后接着填入正下方紧邻的一个方格，再横行向左填，到左端后再折入下边紧邻的一行向右填，如此进行直到填满整个长方形．所得排列如下：

I	M	U	S	T	H	A	V
R	E	H	T	O	N	A	E
H	U	N	D	R	E	D	D
X	X	S	R	A	L	L	O

图 14.1

我们必须知道，而且我们必将知道

http://maths352.bokee.com

假定用竖直换位的方法，从右上角读起，向下读到右下角后从下向上接读紧邻的左边一列，然后又从上向下接读再左边的一列，如此接下去直到读完整个长方形．所得待发的密码信息就是

VEDOL DAAHN ELARO TSTDR SNHUM EUXXH RI.

翻成明码时所需的反转步骤没有什么特殊的困难．

这里要指出，由于国际电报章程规定了拍送电报的费用，密电码的最后定稿通常都分成五个字母一组．从密码分析的角度
[391] 看，这一点是无关紧要的．

上述一类方法的安全性很低，而且也不便于随时变更．即使长方形格子的多少与填入和换位路线都作有规律的变更，敌方也不难破译截获的密电．破译的方法主要是试读，但是由于可能的读法不多，所以稍有经验的人在很短时间内即能破译．

一种广泛采用的路线换位法的变形叫做*列换位法*．在这个方法里所用的几何图形仍是一个长方形，信息的填入是按通常的写法进行的．换位是竖直的，各列的次序由一个数字密钥决定，密钥的长度与长方形的列数相同．例如，假定密钥是 3－2－7－1－4－6－5，信息是 THE PRISONERS HAVE SEIZED THE RAILWAY STATION．

第一步是把信息填入一个长方形格子，每一列格子的上边写上密钥的数码：

3	2	7	1	4	6	5
T	H	E	P	R	I	S
O	N	E	R	S	H	A
V	E	S	E	I	Z	E
D	T	H	E	R	A	I
L	W	A	Y	S	T	A
T	I	O	N			

图 14.2

最好不要用伪码补满长方形的末一行，因为不然会给敌方一个

我们必须知道，而且我们必将知道

http://maths352.bokee.com



探索密钥长度的线索.然后,按照密钥的数码重排各列,接着把 [392]
待发的密电划分成五个字母为一组的电文,即:

PREEY NHNET WITOV DLTRS IRSSA EIAIH ZATEE SHAO

翻译的第一步是确定长方形有几个长列,即,长方表的末一行里有几个字母.它可以用密钥的长度除电文的长度(字母的个数)而得到.相除时的余数就是所要的数.算出它之后,可把密电的字母排到正确的位置上,于是电文即显示出来.

当密钥相当长时,最好不要把它写成书面的,方便的做法是从一个容易记忆的密钥字或词组导出数字序列.这可按多种办法中任一种去做.最普通的做法是按字母的正常顺序予以编号.例如,假定关键字是 CRYPTOGRAPHY.将其中的字母 A 编为 1 号.因为没有字母 B,所以字母 C 编为 2 号.再其次是字母 G,编为 3 号,等等.直到这个关键字的每个字母都编上号为止.如果一个字母出现多次,那么也要给它们像不同的字母一样从左到右予以相继编号.这样得到的整个数字密钥就是

C	R	Y	P	T	O	G	R	A	P	H	Y
2	8	11	6	10	5	3	9	1	7	4	12

破译列换位密码的方法是基于它是以整列字母作为一个整体而进行换位.假定我们要试图破译上边所得的密电.第一步是配合两组在明码电文中常见的连接字母.英文中最常见的双字母组合是 TH,所以我们可以从把每个 T 与每个 H 靠到一起并把每个 H 与每个 T 靠到一起开始.在每种情况下,紧靠 T 或 H [393]
的前边或后边的字也被靠到一起.例如,如果把密电中的第一个 T 与末一个 H 相靠,我们就得到下边的一些组合:

YA
NT
HE
NE
ES

我们必须知道，而且我们必将知道

http://maths352.bokee.com



TH

WA

IO

T

O

每列中应该有几个字母尚且不知道，但所用个别字母的位置有时能提出一些限制．在上边的例子中，第一列最下边的 O 可以丢掉，因为换位长方形的长列较短列多一个字母．紧靠 O 上边的 T 仅当它是密电码最后一个字母时才是正确的，因为它在最后一个长列的末尾．作为说明怎样根据假定去限制列长的例子，假定我们把密电码的第一个 T 与第一个 H 靠到一起，也就是移过三个字母．这样一来只得到三个双字母组合．于是，在这个假定下任一列的长度都不会超过四个字母．

对于每种可能的 TH 组合都会有像上边给出的那样的两列，下一步需要的是由高频组合中根据最佳选择选出一对来．有经验的密码分析员能一看就知道了，不过用纯粹数学的方法也能得到同样的结果．不同的作家已经广泛地研究了单字母、双字母、三字母以及多字母组合的相对频率．这些相对频率可以被看成是相应的明文电码中字母组合的一个不变性质，因为它们是
[394] 从非常大量的电码的研究中得来的．将每个双字母组合的相对频率作为该组合的权重，那么要选出具有最大平均权重（每个双字母组合）的双列就是很简单的事了．

按这样的办法检查的结果表明上边所给的排列已经是一个非常好的排列．仅只 YA 与 WA 不是高频双字母组合，而且前者超出了列的限制．如果假定这个排列是正确的，那么我们就进一步增添一个第三列，或者添在左边或者添在右边，目标在于获得良好的明电码三字母组合．

组合 IO 的后边常常跟着一个 N．此外，组合 TH 使我们联想到单字 THE．这又提醒我们去找一个 E 而且它下边隔着一格

我们必须知道，而且我们必将知道

http://maths352.bokee.com

有一个 N.在这份密电码中我们只找到一处合乎这个要求.注意在已经找到的双字母组合旁增添相应的字母怎样确定了下边的三列：

HEP
NER
ESE
THE
WAY
ION
T

如果有多种可能而不只是一种情况,那就可以再把各种情况中的三字母组的权重加起来进行比较而取平均值最大的一种.在当前的例子中.我们路子显然是走对了,破译在即.

若是知道密电中很可能出现的个别字,则上述步骤可予以大大简化.这种知识在军事密电分析中是很平常的,在其他领域中亦然.事实上,许多密码分析的作者都常常把"可能出现的字"或"直觉"方法当作破译密码的多种方法之一.

以上所说关于破译列换位密码的方法都暗中认为密码分析 [395]
员仅仅掌握一条密电码.前边已经指出,实际上他手中可能有同一密钥管着的许多条密电码可供研究.这时可以试用多种方法迅速完成破译.

其中下边的方法值得注意,因为它适用于任何换位法.假定有两条或多条"同样长"并且由同样的换位法编成的密电码.这时,不管编法有多么复杂,明电码中位置相当的字母在密电码中的位置显然也必是相当的.假定把这些密电码各占一行对齐排到一起,使第一个字母在同一列中,第二个字母同在一个第二列中,等等.这时,如果假定某一条电码中某两个字母在明电码中是相继的,那么其余任一条密电码中相应位置上的两个字母必然按相同的次序结合到一起.于是它们就对最初的假定是否正

我们必须知道，而且我们必将知道

http://maths352.bokee.com

确提供了一个检验办法.同样,列换位法中两列的结合也可供检验该两列中一双特定字母的配合是否正确.在每一个这种双字母组合的旁边可以添上第三个字母而构成三字母组合,等等.这种想法实质上就是把对齐的许多密电码整列地“颠来倒去”,还可以采用求频率和的数学方法而从中得到好处.

选择一个固定的组合例如 QU 或极常见的双字母组合如 TH 或 RE,常常是一个良好的起步.如果双字母组合中的字母之一是不常用的,例如 *VE*,则可能情况就减少很多.给定四条等长密电码的一个最小者,人们肯定能够破译这些密电码.然而,这个破译未必能使密码分析员翻译更多的长度不同的密电码.为此,他必须取得关于通用方法的某些知识和从已破译的密电
[396] 码推出的密钥.

多条密电码的对比分析法 对破译列换位密电码富有成效的另一个方法可以用于破译共同段较多或较长的两条或多条密电码.此种共同段常见于大型通讯装备发送的密电码中,因为在那种场合有采用标准用语的倾向.为了更具体地理解这种方法,让我们用数字密钥 8-6-4-1-5-3-2-7 将下边两条包含共同段 THE FIRST AND SECOND DIVISIONS 的明电码编成密电码.

8	6	4	1	5	3	2	7
W	H	A	T	A	R	E	T
H	E	O	R	D	E	R	S
F	O	R	*T*	*H*	*E*	*F*	*I*
R	*S*	*T*	*A*	*N*	*D*	*S*	*E*
C	*O*	*N*	*D*	*D*	*I*	*V*	*I*
S	*I*	*O*	*N*	*S*			

8	6	4	1	5	3	2	7
T	*H*	*E*	*F*	*I*	*R*	*S*	*T*
A	*N*	*D*	*S*	*E*	*C*	*O*	*N*
D	*D*	*I*	*V*	*I*	*S*	*I*	*O*
N	*S*	W	I	L	L	L	E
A	V	E	A	T	O	N	C
E							

图 14.3

可供密电分析员研究的两条密电码是:

我们必须知道,而且我们必将知道

http://maths352.bokee.com

1. TR*TAD* (1) *NE*R*FS* (2) *V*REE*D* (3) *I*AOR*T* (4) *NO*AD*H* (5) *NDS*HE (6)
*OSO**I*T (7) *S**IE**I*W (8) HF*R**CS*

2. *FS*VIA (1) *SOI*LN (2) *RCS*LO (3) *EDI*WE (4) *IEI*LT (5) *HND*SV (6)
*TNO*EC (7) *TADN*AE (8)

他会注意到斜体字母共同段并在下边画线标明.

注意构成共同段的字母是怎样出现在这两条密电码里的.它被断成小段的段数等于长方形中的列数,每个共同小段上边的数码就是相应的列上边的密钥数码.第一条密电码中的字母 *RCS* 居于它们所在列的下端.它们表明,共同用词是处在相应 [397]
明文电码的末尾.另一方面,字母 *FSV* 居于第二条密电码中它们所在列的顶端,表明共同段是处在相应明文电码的开端.从这点信息立即可以断定每一列的长度.例如,在第一条密电码中,第一列包括字母 TR*TADN*,第二列包括字母 ER*FSV*,等等.在第二条密电码中,第一列包括字母 *FSV*IA,第二列包括字母 *SOI*LN,等等.于是我们就确定了每条密电码中哪些列是长的,哪些列是短的.

除了上述信息之外(它本身就颇有价值),人们几乎总可以从这些共同小段得到密钥的一些片段,有时甚至是整个密钥.为了说明具体是怎样得的.让我们姑且假定已经知道原来的长方形.然后注意字母 T,它是共同小段的第一个字母,出现在第一条密电码的第四列里和第二条密电码第一列里.于是,共同小段的任一字母在第一个长方形里所在的列比它在第二个长方形里所在的列靠右三列.

第二条密电码开端的字母 *FSV* 必在上边标写着密钥数码为 1 的那一列里.第一条密电码的字母 *FSV* 来自上边标着数码 2 的那一列.但是,如果这些字母在第一条密电码里比它们在第二边密电码里的位置靠前三格,那么数字密钥应包含

我们必须知道,而且我们必将知道

http://maths352.bokee.com

序列 1－？－？－2(这里的问号表示待定的数码).第二条密电码里上边标码为 2 的那一列的共同小段是 *SOI*,相应地在第一条密电码里的是上边标着数码 6 的那一列.所以,根据和前边同样的道理,密钥必包含这样的序列:1－？－？－2－？－？－6.第二条密电码的 6 号列相应于第一条密电码的 5 号列.想到密钥的长度为 8,我们现在可以说密钥应包含序列 1－5－？－2－？－？－
[398] 6－？.

继续这样分析下去,我们就建成整个密钥 1－5－3－2－7－8－6－4,它是真正密钥的一种轮换形式.如果将它应用到第一条密电码上,结果将是:

1	5	3	2	7	8	6	4
T	A	R	E	T	W	H	A
R	D	E	R	S	H	E	O
T	H	E	F	I	F	O	R
A	N	D	S	E	R	S	T
D	D	I	V	I	C	O	N
N	S				S	I	O

图 14.4

一看就知道正确的起首字母的所在了.确定循环的起点的另一个办法是注意密电码是怎样断成长列和短列的.由于多一个字的列都在原先的长方形的左端,循环必从紧跟在一个短列后边的长列起始.

从以上示范,读者将会理解由于两个相同段中相应字母的相对位移与密钥的长度是互质的,从而我们能够导出整个密钥.如果这两个数有一个公因子,那么密钥将断为一些子循环,其个数和这两个数的最大公因子相同.于是需要把这些子循环连接成整个循环.这时会得出好几个可能的答案,不过试一下就会判断出哪一个是正确的.

在得到刚才所说的破译时,我们假定了相对位移是知道的.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

有时候的确如此. 例如，考虑结尾相同的两条密电码. 在根据相同段被截成的小段数目确定了密钥长度之后，立即就得到每个 [399]
长方形里长列的个数. 这两个数的差就是所找的位移. 由于在以上研究的两条密电码中，共同段在第一条的开头而在第二条的末尾，这就有可能确定两者之间的相对位移. 又因为共同段的长度是 26 个字母，所以它的最后一个字母必在第二条密电码的第二列中. 而且，这个字母必在第一条密电码的最后一个长列里，即第五列里. 因此，位移是三列.

如果共同段的相对位置是一样的，那么就没有位移，就像当它们都处于密电码的开头那样，这种情况下就不可能用这个方法得到关于真实密钥的任何信息.

当相对位移不确定时，在得到正确的答案之前还需要对每种可能性的假定做为数相对不多的检验.

如果在列换位所成的密电码上再进行第二次列换位，那么安全性就大大地加强了. 这第二步中可以用原来的密钥，也可以换用另一条密钥. 不管是哪一种情况，相继两次列换位的结果都可以由原来的明电码经过单独一次换位而完成，但这个换列步骤要比列换位复杂得多. 此种方法称为*二次换位法*. 用此法编成的单独一个密电码的安全性是非常高的. 但是两条或多条长度相同的密电码则不难按上边所说的方法破译. 如果密码分析员掌握了单独一条密电码及其译文，那么他就能够找到二次换位法里的所有密钥.

作为换位法的第二个例子，我要说几句关于所谓格子窗的

我们必须知道，而且我们必将知道

1	2	3	4	5	1
5	1	2	3	1	2
4	3	1	1	2	3
3	2	1	1	3	4
2	1	3	2	1	5
1	5	4	3	2	1

图 14.5

原来明电码中的字母或数码.这样做的方法之一是去那样安排格子窗的孔眼位置,使当你把格子窗相继放到不同的位置上时,下层纸上的每个小方格都露出一次而被填用.用第二种用法时,孔眼位置是那样安排的,要使下层纸上只有某些小方格能露出来而被填用,这时密码编制者必须在有效字母周围的空格里填上一些"伪电码".一般说来,这是一种非常难破译的方法,同时也有一个缺点,即,编成的密电码比原来的明电码长得多.当然,在格子窗法里,电码的填入和译出可以按任何预先安排的路线进行.

上边画的格子窗是一个具有 36 个小方格的"旋转格子窗"的例子.如果在把它放在任一位置上时露出的小方格填完后就它旋转 90°而继续再填,那么当格子窗转回到原位置后就会发
[401] 现每一个小方格都填上了字母.图 14.5 中小方格里的数码表明了构造的方法.从由小方格组成的每一个同心环圈上都要切掉对应于每个数码的一个小方格.如果一边的方格的数目是奇数,那么格子窗的中心正方形就不要切掉①.

① 这些条件一是为了保证格子窗连成一个整体而不断开,二是为了保证格子窗旋转一周后恰使下层纸上的小方格都露出一次.窗口的开法不是唯一的,图中所示只是一例.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



当通讯的数量较大时，格子窗不是很适用的．此外，它们的安全性也很低．例如，所有用给定的一个旋转格子窗编成的密电码都将断成同样长的一些片段，每一片段都经同样的处理．从而可以适用调换列的办法．

至此所说的换位法里密码处理的单元都是单个的字母．没有理由说不能把单元改换为有规律的字母小组、或音节小组、甚至整个单词．这样的做法并非鲜见．历史上一个突出的例子是1861—1865年美国内战期间联邦军用的对单词的路线换位法，其中专有名称被换为一些等价的字符．有时也用长方格子窗，孔眼相当长，使得整个音节甚至整个单词都能一次填写进去．

替代法　最简单的替代法是永远用相同的字母代表明电码里相同的字母．这可能是最为人熟知的密码类型，恐怕也是初搞密码术的人首先想到的．究竟等价字符采取什么形式，显然是无关紧要的．然而奇怪的是何以许多人总认为采用复杂的任意符号会比采用字母或数码的方法更为安全．

采用此种方法的最简单做法是以"替代字母"的形式列出对照表，"一行是明码"，另"一行是密码"．明码字母在明码行里，用密码行里对照的字母去一一替代它们．

例如，如果用对照表： [402]

明　ABCDEFGHIJKLMNOPQRSTUVWXYZ

密　ADGJMPSVYBEHKNQTWZCFILORUX

则语句 COME HOME ALL IS FORGIVEN 变成密码 GQK-MVQKMAHHYCPQZSYLMN．

通常在编写替代字母表时候，明码行就按"正常"的字母表排写．此时，只需指定密码行就确定了整个对照表．按照密码行构成的方式，对照表可分为三种不同的类型．

1．标准对照表　这里，密码行是正常次序字母表或其"逆序"表的一个轮换的结果．这是所知的最古老的一类对照表．有些作者把采用一种标准对照表的密码编写法称为裘利斯·凯撒

我们必须知道，而且我们必将知道

http://maths352.bokee.com

(Julius Caesar)法.不过,凯撒只是用了许多可能的标准对照表之一,他的密码行总是以字母 D 开始的正常次序字母表①.

2. *系统混排对照表* 采用标准对照表的缺点是明显的.只要鉴别出一两个字母就足以断定整个对照表.为了避免这个缺点并且仍然保持不必列写密码行,必须采用某些系统的方法去改排正常的字母次序.密码术的文献上有许多解决这个问题的方案,但这里只提出一种作为例子来加以说明.让我们选取一个不含重复字母的单字作为密钥,譬如 FISHER.把它填写到一个长方表的
[403] 第一行里,然后把其余的字母按正常顺序填入下边的几行:

2	4	6	3	1	5
F	I	S	H	E	R
A	B	C	D	G	J
K	L	M	N	O	P
Q	T	U	V	W	X
Y	Z				

图 14.6

最后按照以单字 FISHER 为基础的数字密钥以列为单元去改排长方表中的所有字母.所得密码行为

EGOWFAKQYHDNVIBLTZRJPXSCMU

3. *随机对照表* 这种密码行的字母是随机选取的.在这样的序列里已鉴别出的字母对于未明字母的鉴别没有什么帮助.

---

① 关于凯撒的某些通信,雪托尼厄斯(Suetonius)说(第 56 章)si quis investigare et persequi velit, quartam elementorum literam, id est, *d*, pro *a*, et perinde reliqua commutet. 关于奥古斯塔斯(Augustus),他说(第 88 章)quoties autem per notas scribit, *b* pro *a*, *c* pro *b*, *ac* deinceps eadem ratione, sequentes literas ponit pro *x* autem duplex *a*.("如果任何人想研究并弄懂它,请他把 D 换成 A,别的字母也相仿处理.""每当他用密码写的时候,他用 B 代 A,C 代 B,……,但用 AA 代 X.")

我们必须知道，而且我们必将知道

http://maths352.bokee.com

自然，此种序列的缺点就是必须把它全部写出来.

单字母法 仅经单个字母替换的密码的破译法是相当熟知的.它的依据是字母表中各个字母的相对频率和它们的各种组合的相对频率.

在英语中，各个字母、最常见的双字母组合与三字母组合的相对频率表如下：①

E 0.131	R 0.067	F 0.028	G 0.014	Q 0.001
T 0.090	S 0.065	U 0.028	B 0.013	Z 0.001
O 0.082	H 0.059	M 0.026	V 0.010	
A 0.078	D 0.044	P 0.022	K 0.004	
N 0.073	L 0.036	Y 0.015	X 0.003	
I 0.068	C 0.029	W 0.015	J 0.001	

[404]

TH 0.034	ER 0.019	IN 0.014	AT 0.013	HA 0.012
HE 0.026	ON 0.019	ED 0.014	OF 0.013	EN 0.011
AN 0.019	RE 0.017	ND 0.014	OR 0.012	NT 0.011

THE 0.015	HAT 0.003	FOR 0.003	NDE 0.003
AND 0.005	EDT 0.003	ION 0.003	HAS 0.002
THA 0.004	ENT 0.003	TIO 0.003	MEN 0.002

进一步的辅助是：(1)选出元音字母，它们是那些高频而又很少相互结合的字母，从而表明一定的间隔关系；(2)选出不常结合的字母，它们给出一些明电文单字或片语.例如：THAT，WHICH，AS SOON AS，BEGINNING，等等.这些字是根据重复字母之间的间隔从密电码里查出来的，它们的外貌称为字貌

---

① P.Valerio, *De la Cryptographie*, Paris, 1893, pp.202, 204.又见A.Conan Doyle, *The Return of Sherlock Holmes*, Frome, 1924, pp.58—83.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

(word pattern);(3)查寻可能出现的单字,它们常常是对密码分析者很有帮助的.

一旦利用上述几点想法之一鉴定出了那怕是很少的几个字,全部破译就很快了.

双字母法 单字母法的安全性相对地较低,其原因在于明电文中每个字母仅有一个替符.如果我们坚持这个替符不能再代表别的字母,并且希望对于个别字母组合提供补充的替符,那就需要多于26个密码符号了.例如,假定我们采用一个二位数作为一个密码单元,那么就有100个可能的替符;假定我们采用一个双字母组合作为一个密码单元,则可能的替符有676个.引入了补充的密码替符后,就可能用几个“不同的”替符中任一个去代表明电文中的每个字母.如果给每个字母派定的替符的个数和它在明电文中出现的相对频率成正比,则译成的密电码的安全性要比用通常的单字母法译成的密电码的安全性高得多.

不过,要破译它也不是很困难的事.方法是先确定哪些密码组合是相互等价的,从而把密电码转化为单字母法译成的密电.
[405] 为此有两个方法可用:(1)根据频率的研究去发现某些字符和另一些字符以相同的方式相结合.仔细研究所有它们的外貌将能确定代表明电文中同一字母的等价替符;(2)仔细研究重复现象将能揭示同一字母被译成不同密码的那些地方.譬如说,出现的情况是:

11	22	27	75	89	16	31
11	22	27	61	89	16	31
11	22	45	75	82	16	31

结论显然是27与45等价,61与75等价,82与89等价.循此往下深入研究将取得不少信息.不必待到确定很多的替符,密码分析者就可能借助于频率方面的考虑和字形而识别出明电文了.

多字母法 如果在某种密码编制法里,明电文的每个字母由两个或多个密码字符去替换,则称之为多字母法.有时,采用多字

我们必须知道，而且我们必将知道

http://maths352.bokee.com

母法时并不利用可变替符.例如,弗朗西斯·培根(Francis Bacon)的代码就是五字母法,每个明文字母用一个由 A 与 B 组成的五字母组代之.因为这样的小组有 32 个(2^5),所以富余 6 个符号,培根不用它们.莫尔斯电码(Morse code)是代码长度不等的多字母法的一个例子①.

复式字母法 较采用可变替符更有效地压低频率的一个方法是对于同一个明文字母采用多个替换字母.这种方法常称为*复式字母法*,并按照字母是否周期地使用而呈两种非常不同的形式. [406]

作为第一种形式的一个简单例子,假定对照表里每个明文字母对应着随机取来的五个不同的字母如下:

明码		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
密码	1	R	K	S	L	D	P	A	V	E	C	O	G	J	U	B	N	I	F	X	Z	W	H	Y	M	Q	T
	2	J	Y	B	I	W	Q	H	X	D	P	T	F	A	Z	G	O	C	L	S	U	E	K	N	V	M	R
	3	F	K	U	D	N	H	T	A	Z	L	G	Q	Y	R	B	I	J	V	M	O	C	W	E	X	S	P
	4	N	T	Q	I	C	G	S	E	J	O	P	A	W	B	V	U	X	D	L	F	R	H	K	Z	M	Y
	5	K	E	M	A	J	B	T	L	V	D	N	U	F	S	C	Q	G	O	X	I	P	Y	W	Z	R	H

图 14.7

将明电文写在五列里,用第一行密码替换明文的第一列里相应的字母,用第二行密码替换明文的第二列里的字母,如此等等.这种步骤进行的结果是第 a 行密码替换的明文字母在明电文中的位

① 这里列出莫尔斯代码表以供不熟悉它的读者参考:

A · –	G – – ·	M – –	S · · ·	Y – · – –
B – · · ·	H · · · ·	N – ·	T –	Z – – · ·
C – · – ·	I · ·	O – – –	U · · –	
D – · ·	J · – – –	P · – – ·	V · · · –	
E ·	K – · –	Q – – · –	W · – –	
F · · – ·	L · – · ·	R · – ·	X – · · –	

我们必须知道，而且我们必将知道

http://maths352.bokee.com

[redacted]

置是第 $5k+a$ 个.按照上列对译表,明电文 THREE SHIPS SAILED TODAY 就被译成密电文 ZXVCJXXZUXXJZAJLUBIKQ.

双密钥法 对照表可以那样安排,用密钥字的规律交换而改变每个明文字母替换的个数,这样,它就不再是固定不变的了.现在就来说明一个这样的做法.老一代的作家对它都有所阐述,其中有些人称之为双密钥法.例如,用一个密钥字 COPYRIGHT 构造下表,即一个所谓维热奈阿(Vegenère)正方表(图 14.8).正方表上边按正常顺序排列的一行字母是明文字母行.如果把正方形的每一行都当作一个密码行,最上边按正常顺序排写的一行为明码行,则图 14.8 实际给出 26 个替换表.让我们

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z
Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X
X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W
W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V
V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U
U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S
S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q
Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N
N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M
M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L
L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K
K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F	J
J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E	F
F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D	E
E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B	D
D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A	B
B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T	A
A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H	T
T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G	H
H	T	A	B	D	E	E	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I	G
G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R	I
I	C	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y	R
R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P	Y
Y	R	I	C	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O	P
P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C	O
O	P	Y	R	I	G	H	T	A	B	D	E	F	J	K	L	M	N	Q	S	U	V	W	X	Z	C

图 14.8

我们必须知道，而且我们必将知道

http://maths352.bokee.com

用正方形中最左边的一列里的字母分别称呼其所在行.然后再用第二个密钥字——AUGUST——去选取采用的行以及采用次序.第一行是 A 行,用它去替换明文中第 $6k+1$ 个字母;第二行是 U 行,用它去替换明文中第 $6k+2$ 个字母,如此等等.得到的 [407]
密电码将是一个六字母式的,不过其中只有五个不同字母.依照上述两个密钥字替换明文 NEED REINFORCEMENTS AT ONCE 的结果将是密电码 VZBXD EMTDA DBFHB TFCAJ STVE.

周期式复式字母法 破译此类密电的第一步是确定每个明文字母可被几个密码字母替换.为了说明怎样解决这个问题,假定有一个字母在密电中重复了多次.如果这个字母的两次出现和密钥的相对位置相同,那么它们将产生相同的密码电文.如果两次出现和密钥的相对位置不同,那么产生的密码电文也必不同.因此,分隔重复密电字码的间隔应是密钥长度的倍数.密钥 [408]
的真实长度是所有此类重复字母的间隔的最大公约数.于是,如果把密电文写成列数与密钥长度相等的长方块,那么在同一列中的明文字母都是按同一行密码译制成的.

第二步是分析这些不同的单字母替换,其步骤与破译前述单字母法密电基本相同.如果有些字母相同,可用统计法结合相应的频率确定之.此外,如果不同的字母有维热奈阿正方形里那样的关联,那么还可以利用某些对称性而从中得到好处,于是识别出一个字母就同时识别出了其他字母.

为了密电码的编制与破译,晚近在密码机的制造方面已做了不少研究工作.其中大部分用的是周期复式字母法.最新的机器是电动的,并且在许多情况下的周期都是大得惊人的数字.此外,独立字符的个数往往与周期是同一数量级的.这些机组比手工快得多也准确得多.它们甚至还可以把打印与发送装置连接在一起,从而编制密电时,既能将密电文保留下来又能将它随即就发送出去;在接到密电后立即进行破译与翻译,一切都是自动的.就当前的密码分析方法而论,由某些此类机器编制的密电码

我们必须知道，而且我们必将知道

http://maths352.bokee.com

实际上几乎是不能破译的.

非周期的复式字母法 这种研究将导致非常复杂的密码分析,所以这里只叙述两个这种例子.

1. 假定已经构造了一个维热奈阿正方形,它有26个不同的密码行,每行由一个字母作标号.于是明文信息本身的字就可
[409] 以当作密钥.例如,假设预先约定第一个密码行是 A 行,那么明电文第一个字母就按这一行译成密码.此后,明电文中每一个后继字母按明电文中前一个字母为标号的密码行译成密码.此法称为自动密钥法.按以单字 COPYRIGHT 为基础的维热奈阿正方形,明文信息 BRIDGE DYNA MITED 被转换成密电码 BOETM BKALN UZXEK.

2. **流动密钥法** 此法除了密钥与信息迥然无关之外,和上述方法是相仿的.此法中的密钥可以是教科书上或期刊上预先规定的某页某行开始的文字.或者,也可以是随机取定的一些字母,而每个通信员都要有它的一个副本.

从实践的角度看,像上边所说两个非周期法中的前一个那样的方法都有一个严重的缺点.万一在信息中发生了一个不管是什么原因引起的错误,使得收到的密电中有一个字母是错误的,那么每个后继字母都会受到影响.由于仅仅在信号的传输中发生错误的平均数就可能高达5%,这就使得识读一条密码信息很困难了,有时简直是不可能的.

复式字母法之所以能够提高安全程度根本上是由于它们压低了用单字母法时的频率.但是如果密码分析者能找到办法把密电分拆成一些单字母组成部分,那么频率的明显差异还会出现.如果密码处理的单元是单个字母,像以上所说的各种替换法那样,那么这种可能性总是存在的.于是人们就想到字母组替代法——用同样多个字母的密码组去替换明电文字母组.

作为第一个例子,我们给出古典的双字母法,即所谓公允式密码.在这个方法中,在由25个小方格组成的正方形格子里,按

我们必须知道，而且我们必将知道

http://maths352.bokee.com

预定的方式填入25个字母(略去一个字母,譬如说,Q).下边所给的正方形里填写的是以单字MAHCHESTER为基础的一个系统混合序列. [410]

M	A	N	C	H
E	S	T	R	B
D	F	G	I	J
K	L	O	P	U
V	W	X	Y	Z

图 14.9

先将明电文字母分成两两一组.为了避免同--组里的两个字母相同,凡遇这种情况时都加入一个假字母,譬如Z.照这样办时,假定明电文的第一个字是BATTALION,它就被分截成为BA TZ TA LI ON.在译成密码时,如果一个双字母组中两个字母出现在正方形表中同一条水平(或铅垂)线上,那么这两个字母的每一个都用正方形表中紧靠在它右边(或下边)的字母去替换,每行和每列中的字母都被看成是循环的.如果一个双字母组中的两个字母不出现在同一行或同一列里,那么它们必定出现在某个长方形的两个对顶点上,这时就用该长方形的另两个对顶点上的字母去替换它们,每一个被处于同一水平线上的那个字母所代替.例如,明文信息WILL MEET YOU AT NOON将先被分截成WI LZ LM EZ ET YO UA TN OZ ON.按照上边所示的正方形表,信息就被译成密电码YFUWK ABVSR XPLHG TUXXT.

这种方法的安全性,说实在的,任何双字母法的安全性都是相当低的.明电文双字母的相对频率有足够大的差异使密码分析者单从频率方面的考虑就能够取得大量的信息.只要正确地鉴别出不多几个双字母组就足以保证破译了.此外,密码分析者还能够尽量利用可能的字和可能的字型.当然,对于后者他只能限于以双字母组为基础的字貌.例如:*RE* FE *RE* NC E, P *RE*

我们必须知道,而且我们必将知道

http://maths352.bokee.com

PA *RE*, *DE* Cl *DE*.

在公允式密码里还有进一步事实可资辅助破译. 如果已经断
[411] 定了 BN 替换的是 TH,那么,NB 替换的就是 HT. 一般地,如果 $A_1A_2 = B_1B_2$,那么 $A_2A_1 = B_2B_1$. 此外,如果已知四个字母 A_1, A_2, B_1, B_2 是位于一个长方形的四个顶点上,那么立即得到额外的判定:$B_1B_2 = A_1A_2$; $B_2B_1 = A_2A_1$. 这些事实在特殊的频率研究中是相当有用的. 例如,在辨别一个高频双字母组合例如 TH(它的倒排 HT 是非高频组合)和另一个如 ER(它的倒排 RE 是高频组合)是否等价的时候. 可以指出,在公允式密码的情况,只要鉴别出不多几个字母就能够复制出整个正方形格子中字母的排法.

当加密处理单元的大小增加时,字母组替代法的安全性提高得很快. 当单元增到五六个字母时,安全性是很高的. 可惜此时也产生了严重的缺点. 密码小组中一个字母之差就会使译出的明电文的整个单元都是错误的,事实上它立即歪曲了五六个字母. 由于对这种密电码不可能引入纠正错误的办法,所以发送一条电文时只要有四五个错误就会使整个电文无法识读了. 这个缺点是要命的. 不过,从理论的角度来看,这种方法是颇有趣的,莱斯特·希尔(Lester S. Hill)教授已经给出了一套非常一般的数学处理①.

代码法 在以上所说的各种密码编制法里,密电文的长度至少和明电文的长度一样长. 主要都是从秘密性的角度考虑的,而不曾从经济方面加以考虑. 但是这方面的考虑常常是首要的,并且促进了称为代码(code)的非常特殊的替换系统的发展. 这时每个通信员都发给一个代码本(code book),其中载有很长的对照表,表里包括着许多单字、词组和句子,旁边对列着任意给它派定的代码. 这些代码常常是由五个字母构成的小组,不过,

---

① American Mathematical Monthly, 1931, Vol. XXXVIII, pp. 135—154.

我们必须知道，而且我们必将知道

http://maths352.bokee.com

有时也采用较少字母构成的有规律的小组，偶尔也采用数码小 [412]
组．还有一些为了拼写出“字典”中未载的字而作的补充约定，它们给单个的字母和常出现的音节分别规定了同义码．

通常一种代码本是为某一特定行业或为一群有特殊兴趣的人而编写的，因而常用的较长的词组、甚至整个句子都包括在这个本子里而被一个代码组所代替．结果，一条密电码常常只有相应明电文的四分之一或五分之一那样长．

作为例子来看一看，下边转录西方旅游者联合会的电缆代码本里标题为 *ARRIVAL* 的一段：

ADAUX	正在等候……的到达
ADAVY	顺利到达
ADAXA	顺利到达，来函由……转交
ADBAE	顺利到达，来电由……转交
ADBEI	顺利到达，旅途愉快，通知朋友们
ADBIM	顺利到达，旅途愉快，
	等等．

这种浓缩法也有它的弱点，一组代码的错误就会失掉相当长的一段明电文．为了避免电文重复的必要性，有预防的措施以纠正错误．具体地说就是从一个特殊的代码构造表里①选取代码小组，这样就保证了每个代码组和另一个代码组至少有两个字母不同．这样一来，一个代码组就可以由它的任何四个字母完全确定．于是，如果在传输中弄错了一个字母，结果在代码本中就查不到这个代码组，于是译电员就知道出现了一个错误．轮流
把每个字母当成一个错误的字母，就可以给弄错的字查到至少 [413]
五个可能的译法，根据上下文就可以选出正确的译文．这个方法

---

① 在 W.F.Friedman 与 C.J.Mendelsohn 的一篇论文里可以找到一个这种表和关于密码的某些有趣注记，见 American Mathematical Monthly，1932，Vol．XXXIX，pp．394—409．又见 p．275．

我们必须知道，而且我们必将知道

http://maths352.bokee.com

的根据是假定收到的代码组中只有一个字母错了.幸运的是,事情几乎总是这样.

代码字构造表的进一步改进是保证代码本中任何两个字的差别不能只是两个字母交换了位置,这有助于校正错误.这种特点是必要的,因为有些秘书,特别是打字员在快速工作时常常不知不觉地发生此类错误.

用代码进行通信时,保密性主要取决于外人能否获得代码本.但是通常规定了代码本是不许从合法持有者手中泄露出去的,譬如,抄录或照相复制都是禁止的.如果有任何泄露的可能,就必须要*超级加密*(Superencipherment),即,把按代码本译成的电文当作明电文看待,再将一种或多种可能的密码编制法应用到代码本上.所用的方法和特定密钥都可根据需要而经常更换.

密码类型的判定 前边已曾指出,在大多数密码分析的研究中都假定了敌方已经掌握了密码的通用类型.当然,情况并非总是如此,而密码分析者也就时常面对着如何判定手中的一组密电是用哪一类方法编成的.它是这个领域中最困难的问题之一.为了不至于使得当前的讨论过分复杂,仅就"当只涉及一种方法时"稍谈几句鉴别密码类型的方法.给定一组要研究的密电,第一步就是系统地查寻其重复性并且研究密电的外貌.如果我们限于研究长度至少为五或六个字母的重复现象,那么就有把握可以说甩掉了任何偶然发生的重复字.假定已经找出了所
[414] 有出现的重复现象的长度并且它们之间的间隔都是同一个数 n 的各种倍数,那么密码的类型可能是多字符的、字母组的或者是代码的.

如果把所有发生的 n 个字母组成的小组都排成一个表,并且作出它们的频率分布,那么我们就能够进一步鉴别这三种类型如下:一个不采用可变替符的多字母法的密电将包含至多 26 个不同的小组,它们各自的频率相当于明电文中各个字母的常态频率.如果采用了可变替符,则可按前述方式确定其等价字母

我们必须知道，而且我们必将知道

http://maths352.bokee.com

而鉴别之.代码型与字母组型的区别在于代码型的 n 个字母组成的小组的形状和结构都是有规律的,小组之间总有两个字母不同,并且可以纳入一个代码字构造表里,表的容量限制着小组的总数.不同的是,在字母组类型里,“每一由 n 个字组成的组合”都是一个真正的密电码小组.从手中一批密电码真正得到的此种小组的个数和这么多的电文里可望出现的明文 n 字母相异小组的个数属于同一数量级.

如果密码单元不是由两个或多个字母组成的小组,那么密电就是单字母型的,并且必是换位型的或者替代型的.如果是换位型的,那么它只不过是原电文中字母的一种轮换,而每个字母的相对频率和在明电文中是一样的.所以,元音字母所占的比例也和明电文中相同,即,大约 40%.由于换位法倾向于把单字断开并把各个字母散布到整个电文里,所以长段的重复即使有可能出现,那也是极少见的.

如果密电不是换位型的,那么它必是替代型的.在替代型的密电文中,各个字母的频率的相对大小和明电文中相同并且变动的程度也相同.这种密码与前者的显著差别是明电文中的低频字母在密电文中呈现为高频字母,而明电文中的高频字母在 [415]
密电文中却呈现为低频字母.由于在明电文中元音字母都是高频字母,所以密电文中元音字母的比例一般地都较明电文中元音字母的比例小.还有,在单字母替代型的密电文中含有相当多的重复,因为明电文中的每个重复都反映到密电文中了,并且这些重复包含着可辨识的字貌.当然,它们之间的间隔没有公因子.

如果基本类型是一种复式字母替代型,则频率分布将会是相当“平坦”的,即,各个密码字母的频率是大致相等的.这是由于采用多个字母而产生的效果,因为这时一个特定的密码有时候用来代表明电文中的一个高频字母而另一些时候又被用以代表明电文中的一个低频字母.剩下的是需要确定这些字母的应

我们必须知道，而且我们必将知道

http://maths352.bokee.com

用是周期地呢还是非周期地.如果它们是被周期地使用着,那么重复之间的间隔将是周期的各种倍数.当电文被断成长度等于周期的小段并且把这些小段并排起来时,每一列中的字母将构成一个单字母替换表.反之,如果各种重复之间的周期没有公因子,那么这个密电文所属的复式字母替代型是非周期的替代.

着眼于破译而对这些类型的进一步研究取决于遇到的是具体哪种类型,以及具体情况下所得可供密码分析者借用的有关信息其他要素.

几点最后的注记 在大多数情况下,一组密码所含的信息只在很短的时期内是有价值的.事实上,通常认为一种密码规律只要能使敌方在破译它时所花的时间长于信息的有效期,那么这种规则就是足够安全的了.不过,有时会发生那样的情况,应用密码分析的原理会得到有一定重要历史价值的材料.例如,第
[416] 一类材料是古代文字.顾名思义,这些材料本来不是什么"保密"文件.但是当人们试图阅读它们时却不得不把它们当作秘密文件看待.另一方面,有时历史学家们对阅读许多年前的秘密信件非常感兴趣.这方面的例子可以举出美国南北战争时期发送的外交密电.

即使在今天,上述两方面的材料也还有许多可供研究.属于古代文字的突出例子是"玛雅象形文字".诚然,对于它们的识别已经取得了很大的进展.专家们已经识别出了玛雅文化里的数字、历法符号,以及表示各个玛雅神祇的象形文字等等.但是还有大量的工作待做.

最后,不妨提及试图破译那种密码的例子——它的存在性本身就是一个疑问.我们可以特别指出,关于培根①与莎士比亚的争论所做的一切工作.用不着多少密码分析的常识就可以看出,已经得到的结果完全是主观的.任何两个独立的研究者应用

① 指 Francis Bacon.——译者注

我们必须知道，而且我们必将知道

http://maths352.bokee.com



现有的方法都不会得出完全一致的结论.一个研究者很可能抱住一种想法缠住不放而力图证明其有效,实际上不过是选用了一种充分灵活的规则以至于想要什么样的结果就可以得出什么样的结果.纽博尔德(W.R. Newbold)教授的案例[①]就是这种现象的一个可悲的例子,他以为自己已经读懂了威尔弗里德·沃伊尼克(Wilfrid M. Voynich)手稿.那是沃伊尼克大约于1912年在意大利发现的一篇二百多页长的中世纪的论文,其书法秀丽而且插图甚多.事实上,它依然是提向语言学家和密码分析家的一份高强的挑战书. [417]

附录:进一步研究的参考资料

BAZERIES, ÉTIENNE

Les chiffres secrets dévoilés, Paris, 1901

Encyclopaedia Britannica

"Codes and Ciphers"

FIGL, ANDREAS

Système des chiffrierens, Graz, 1926

GIVIERGE, COL. MARCEL

Cours de Cryptographie, Paris, 1925

GRANDPRÉ, A. DE

La cryptographie pratique, Paris, 1905

LANGE, ANDRÉ, and SOUDART, E. A.

Traite de Cryptographie, Paris, 1925

LANGIE, ANDRÉ

De la cryptographie, Paris (英译本 J.C.H.Macbeth, Cryptography, New York, 1922)

---

① The Cipher of Roger Bacon, Philadelphia, 1928. 在不列颠博物馆和纽约公共图书馆里都有沃伊尼克手稿的照相副本[它已不再归于R·培根(Bacon, R.)].

我们必须知道，而且我们必将知道

http://maths352.bokee.com


[redacted]

SINKOV, ABRAHAM
Elementary Cryptanalyis, New York, 1968
VALERIO, P.L.E.
De la Cryptographie: Part I, Paris, 1893; Part II, Paris 1896
YARDLEY, HERBERT O.
[418] The American Black Chamber, Indianapolis, 1931

我们必须知道，而且我们必将知道

http://maths352.bokee.com

索引

A

Abel, N.H. 阿贝耳 62
Aces paradox 幺的悖论 44
Agrippa, Cornelius 阿格里帕 194
Ahrens, W. 阿伦斯 194
Aitken, A.C. 艾特肯 x, 46, 386–387
Aix, labyrinth at 艾克斯迷宫 258
Alcuin 阿尔昆 3, 118
Alexander, J.W. 亚历山大 232
al Kashi, J.M. 阿尔卡西 352
Alkborough, labyrinth at 阿尔克波罗迷宫 259
Alphabet, Morse 莫尔斯字母 406
Ampère, A.M. 安培 364
Anallagmatic pavements 半条反拼砌 107–109, 274
Analysis situs 拓扑学 222–270
Anaxagoras 安纳克萨戈拉斯 350
Anderson, A 安德森 65
Andreas, J.M. 安德烈斯 vii, 128, 154, 171, 215, 239
Andreini, A. 安德烈尼 147, 160
Andrews, W.S. 安德鲁斯 194, 212
Anning, N. 安宁 171
Antipho 安蒂福 350
Antiprism 拟棱柱 130
Apollonius 阿波罗尼奥斯 340, 343, 351
Appel 阿佩尔 224
Arago, F.J.D. 阿拉戈 372
Archibald, R.C. 阿奇博尔德 65
Archimedean solids 阿基米德体 136–140, 159
Archimedes of Syracuse (锡拉丘兹的)阿基米德 340–343, 347, 350
Archytas, on Delian problem 阿尔希塔斯，论德利安问题 341
Arithmetical fallacies 算术谬论 41–45
Arithmetical prodigies 算术神童 360–387
Arithmetical puzzles 算术趣题 4–50
Arithmetical recreations 算术游戏 3–75, 312–337
Arithmetical restorations 算式复原 20–26
Arnoux, G. 阿尔诺 206, 210
Arya–Bhata 阿耶波多(即，圣使)

我们必须知道，而且我们必将知道

http://maths352.bokee.com

88,351
Asenby, labyrinth at 阿森比迷宫 259
Augustus 奥古斯塔斯 403
Auto – key system 自动键系统 410
Axis of symmetry 对称轴 131,135

B

Bachet's problemes 巴协的问题 xi、3,5,6,7,8,9,11,12,13,17,18,19,28,30,33,50,51,52,118,326,328
Bacon, F. F·培根 406,417
Bacon, R. R·培根 417
Baker, H.F. 贝克 323
Ball – piling 堆球 149 – 152
Ball, W.W.R. 鲍尔 vi
Barbette, E. 巴尔贝特 212
Barrau, J.A. 巴罗 108
Baudhayana, on π 鲍德海雅纳,论 π 351
Bazeries, E. 巴泽瑞斯 418
Belevitch, V. 别列维奇 308
Bell, E.T. 贝尔 57,61
Bennett, G.T. 本内特 68,81
Benson, W.H. 本森 213
Bergholt, E.G.B. 贝霍尔特 49,211
Berlekamp, E.R. 伯利坎普 303
Bernoulli, John. J·伯努利 41,349
Bernoulli, N. N·伯努利 50
Bernoulli numbers 伯努利数 71
Bertrand, J.L.F. J·L·F·贝特朗 41
Bertrand, L. L·贝特朗 177
Berwick, W.E.H. 贝维克 23
Besicovitch, A.S. 别济科维奇 100,101
Bewley, E.D. 比利 49
Bhaskara, on π 巴斯卡拉,论 π 352
Bidder, G.P. 比德 367 – 372,378 – 386
Bidder family 比德家族 371 – 372
Biering, C.H. 比林 339
Bilinski, Stanko 比林斯基 143,300
Bilguer, von, on chess pieces 比尔格论棋子 165
Birkhoff, G. 伯克霍夫 73
Binet, A. 贝尼特 375
Birthdays problem 生日问题 45
Bishop's re – entrant path 象的回路 187
Block design 区组设计 276,293
Bloom 布卢姆 101
Bordered magic squares 镶边幻方 200
Bolyai, G. 波尔约 89,106,161,280
Bose, R.C. 玻色 292,302
Bouniakowski, V., on shuffling 布尼亚科夫斯基论洗牌 323
Bourlet, C.E.E. 博莱特 31
Bouton, C.L. 布顿 37
Bouwkamp, C.J. 鲍坎普 113,116
Brahmagupta, on π 婆罗摩笈多(印.梵藏),论 π 351
Brassine 布拉辛尼 67,72
Breton, on mosaics 布雷顿,论嵌花 258
Brillhard, J.D. 布里尔哈德 62,66
Bromton 布朗姆顿 256
Brooks, R.L. 布鲁克斯 116

我们必须知道，而且我们必将知道

http://maths352.bokee.com



Brouncker, V., on π 布龙克尔,论π 355
Brown, B.H. 布朗 27
Bruck, R.H. 布鲁克 311
Brückner, M. 布吕克纳 147
Brun, V. 布伦 62
Bryso 布赖索 350
Busschop, P. 巴斯乔普 89
Bussey, W. 伯西 282
Buxton, J. 巴克斯顿 361 - 364

C

C-matrix C矩阵 308
Caesar, J. 凯撒 403
Calculating prodigies 计算神童 360 - 387
Calender problems 日历问题 26
Callet, J.F. on π 卡莱,论π 357
Cantor, M., on π 康托尔,论π 349
Cardan, G. 卡尔丹 3,318,320
Cards, problems with 纸牌问题 18 - 20,47,49,191,322 - 337
Cartwright, W. 卡特赖特 389
Cauchy, A.L. 柯西 145,372
Cayley, A. 凯莱 146,223,238,261,336,355
Cazalas, J.J.A.M.E. 卡扎拉斯 213
Cells of a chess - board 棋盘的格子 162
Ceulen, van., on π 范·雪伦,论π 353,355
Characteristic, Euler - Poincaré 欧拉庞加莱示性数 233
Chalk, J.H.H 乔克 ix
Chandler, D. D·钱德勒 ix
Chandrasekharan, K. 钱德拉塞卡兰 40
Charcot, J.M. 沙尔科 375
Chartres, R. 沙特尔 41,83,359
Chasles, M., on trisection of angle 沙勒,论三等分角 346
Cheney, W.F.Jr. 切尼 94
Chernik, J. 切尔尼克 211
Chess 棋:
Number of initial moves 起始步数 163
Maximum pieces problem 最大棋子数问题 172
Minimum pieces problem 最小棋子数问题 172
Chess - board 棋盘:
Games on chess-board 棋盘上的游戏 124 - 127,162 - 192
Knight's move on chess-board 棋盘上的马步 175 - 186
Chess - board, notation of 棋盘格子的标号 162
Chess pieces, value of 棋子的威力 163 - 165
Chifu - Chemulpo puzzle 奇夫切马尔波难题(即,错车问题) 117,129
Chilton, B.L. 奇尔顿 143
Chinese rings 九连环 318 - 322
Chronicles 克朗尼克尔斯 350
Chrystal G. 克里斯托尔 41,57
Ciccolini, T., on chess 奇科里尼,论棋 181

我们必须知道，而且我们必将知道



Ciphers 密码 388-418
Cissoid 蔓叶线 341,343
Clairaut, on trisection of angle 克莱罗，论三等分角 346
Claus, M. 克劳斯 316
Clausen, on π 克劳森，论π 357
Close-packing, hexagonal 六角形密装 151
Close-packing, spherical 球体密装 149
Coins of Cnossos 克诺索斯钱币 257, 258
Coccoz, M. 科克兹 78,212
Code, Morse 莫尔斯电码 406
Code-book, ciphers 代码本 412-414
Colburn, Z. 科尔伯恩 365-370, 375,378,381,384
Colebrooke, H.T. 科尔布鲁克 351
Cole, F.N. F·N·科尔 65,281
Cole, R.A.L. R·A·L·科尔 335
Collini, on Knight's path 科尔里尼，论马路 181
Collins 科林斯 356
Colour-cube problem 染色立方体问题 113
Colouring maps 地图染色 222-242
Combinatorial designs 组合设计 271-311
Compass problems 罗盘问题 96
Compound polyhedra 复合多面体 134,136,146
Conchoid 蚌线 341,345
Conics 圆锥截线 346
Continued fractions 连分式 55,58,86
Contour-lines 等高线 238
Convergents to a continued fraction 收敛于一个连分式 56,58,87
Conway, J.H. 康韦 308
Coolige, J.L. 库里奇 46
Coxeter, H.S.M. 考克斯特 vii,39, 57,99,143,152,159,237,280,296, 304
Cramer, G. 克莱姆 45
Creation, the 创造世界 66
Cretan labyrinth 克雷顿迷宫 258
Cryptography and cryptanalysis 密码术与密码破译 388-418
Cube, duplication of 二倍立方体 93,339-344
Cubes, magic 魔方 217-221
Cubes, skeleton 立方骨架 48,295
Cuboctahedron 八芒星 137,147
Cummings, L.D. 卡明斯 281
Cunningham, F. 坎宁安 101,102
Cunningham, F.Jr. 小坎宁安 ix
Cusa, on π 库萨，论π 353
Cutting cards, problems on 切牌问题 19
Cyclotomy 割圆术 94-96

D

D'Alembert, J. 达朗贝尔 43
Darboux, G. 达布 376,378
Dase, J.M.Z. 达泽 357,372-374
Davenport, H. 达文波特 45,108
Davis, C. 戴维斯 267
Davoust 达武斯特 27

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Decimals 十进制小数 53 – 55
Decimation 十一抽杀 32 – 36
De Coatpont 德·科特庞特 89
De Fonteney, M., on ferry problem 德·丰特内,论摆渡问题 119
De Fouquières, B. 德·福基埃 104
De Grandpré, A. 德·格昂普雷 388
De Haan, B. on π 德·哈恩,论 π 349,354
Dehn, M. 德恩 93
De Lagny, on π 德·拉尼,论 π 356
De la Hire, P. 德·拉·伊尔 202,203
De la Loubère, S. 德·拉·卢拜尔 195,196,204 – 205,207
Delannoy, M. 德兰努瓦 119,123
De Lavernède, J. E. T. 德·拉韦奈德 182
Delens, P. 德连斯 21
Delft 代尔夫特 22
Delian problem 德利安问题 93, 339 – 344
Deltoid 三尖形 100
De Lury, D. B. 德·勒里 44
Dembowski, P. 登博夫斯基 311
De Moivre, A. 德·莫瓦弗尔 175,176
De Montmort, P. R. 德·蒙特摩 2, 46,175
De Morgan, A. 德·摩根 223,347, 349,359
Denary scale of notation 十进制记数法 10 – 17,20 – 26,53
De Parville, on Tower of Hanoi 德·帕尔维伊,述河内塔 317
De Polignac, A. 德·波利尼亚克 64,184
Derangements 重排 46,337
Derrington, on queens problem 德灵顿,论多后问题 171
De St. Laurent, T. 德·圣洛朗 323
Desargues configuration 德沙格构形 305
Descartes, R. 笛卡儿 343,344, 346,356
Diabolic magic squares 魔幻方 203, 206,208 – 212
Diamandi, P. 迪亚曼狄 375,377
Dice, cubic and octahedral 骰子,正方体的与正八面体的 214
Dickson, L. E. 迪克森 67,69,73, 279,332
Digital process 和码法 381
Digits, missing 丢失的数码 20 – 26
Diocles, on Delian problem 狄俄克利斯,论德利安问题 343
Diodorus, on labyrinth at Lake Moeris 狄奥多洛斯,述美利斯湖边的迷宫 256
Diophantine equations 丢番图方程 69
Dirichlet, L. 狄利克雷 71
Dissection problems 剖分问题 87 – 94
Dodecahedron, great 大十二面体 145,234
Dodecahedron, pentagonal 十二-五角形面体 *132,231,235,262 – 263*
Dodecahedron, rhombic 十二菱面体 137,150

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Dodecahedron, stellated 十二星形面体 144
Dodgson, C. L., on parallels 道奇森，论平行线 77
Dominoes 骨牌(即，多米诺骨牌) 31, 214, 251 – 254
Donchian, P. S. 唐奇安 vii, 141
Double transposition 二次换位 400
Doubly – magic squares 二重幻方 212
Dragon designs 龙纹图案 266 – 270
Drayton 德雷顿 256
Dual maps 对偶地图 234
Dudeney, H. E. 杜德尼 35, 39, 49, 59, 88, 92, 96, 116, 118, 127, 187, 189, 211, 214
Duijvestijn, A. J. W. 杜伊维斯蒂茵 116
Duplication of cube 二倍立方体 93, 339 – 344
Dürer, A. 丢勒 194, 202

E

e 47, 56, 87, 348
Eckmuhl 埃克米尔 27
Eddington, A. S. 爱丁顿 69
Eden, M. 伊登 75
Eichler, M. 艾希勒 75
Eigenvalue 本征值(即，特征值) 302
Eight queens problem 八后问题 166 – 171
Eisenlohr, A. 艾森洛尔 (著古埃及数学手册) 350
Enneacontahedron 九触面体 143
Equilateral zonohedra 等边环带多面体 141
Elements, the four 四行 133
Enantiomorphous pair 配对 129, 135, 139, 147, 159, 215, 238, 241
Enciphering and deciphering 译密与译解 390
Encke, J. F. 恩克 373
Eneström, G., on π 恩内斯特勒姆，论 π 349
Equiangular lines 等角线 299
Eratosthenes 埃拉托斯特尼 340
Erdös, P. 爱尔特希 63
Error – correcting code 纠错码 274, 297
Escott, E. B. 埃斯科特 214, 358
Estermann, T. 埃斯特曼 64
Etten, H. van 埃滕 12
Euclid 欧几里得 60, 66, 76, 83, 96, 97, 110, 132, 139, 280, 350
Euclidean construction 欧几里得作图法 95 – 97, 139, 338
Euler, L. 欧拉 58, 61, 66, 68, 70, 175 – 179, 203, 290, 349, 356
Eulerian cubes 欧拉立方 192, 219
Eulerrian squares 欧拉方 190 – 192, 212, 290
Euler's formula 欧拉公式 132, 146, 229, 233, 238
Euler's formula, proof of 欧拉公式的证明 232 – 233
Euler's officers problem 欧拉的官员问题 192
Euler's unicursal problem 欧拉的单行

我们必须知道，而且我们必将知道

http://maths352.bokee.com

线问题 243－247
Euzet, M. 欧泽特 89
Exploration problems 拓荒问题 32

F

Factorization 因子分解 61,62
Fano, G. 法诺 282
Federico, P.J. 费德里科 115
Fedorov, P.J. 费多罗夫 141－143
Feller, W. 费勒 324
Ferguson, D.F., on π 弗格森,论 π 358,386
Fermat numbers 费马数 xii,67,94
Fermat's criterion for primes 费马的素数判断法 61
Fermat's Last Theorem 费马最后定理 69－73
Ferry－boat problem 摆渡问题 118－120
Fibonacci numbers 斐波那契数 57,86
Fifteen puzzle 华容道(即,十五子戏) 312－315
Finite affine plane 有限仿射平面 283
Finite projective plane 有限射影平面 284
Fisher, R.A. 费希耳 192
Fitzpatrick, J. 菲茨帕特里克 122
Five－disk problem 五圆覆盖问题 97
Fonteney, on ferry problem 丰特尼,论摆渡问题 119
Foote, R.M. 富特 ix
Foucault 傅科 102
Fouquières, B. de, on games 富基埃,论博弈 104
Four－colour conjecture 四色猜想 222－231
Four "4's" problem 四个"4"的问题 16
Four digits problem 四个数码的问题 15
Fourrey, E. 富雷 27
Fox, Captain, on π 福克斯上尉,论 π 359
Frankenstein 弗兰肯斯坦 x
Franklin, P. 富兰克林 230,237
Frederick 弗雷德里克 223
Frènicle de Bessy, B. 弗雷尼克尔 200
Friedman, W.F. 弗里德曼 413
Frieze 弗里兹 11
Frost, A.H. 弗罗斯特 203
Fuller, T. 富勒 365

G

Gabard 伽巴德 66
Gale, D. 盖尔 32
Galois fields 伽罗瓦域 73－75,107,191,219,282
Galton, F. 高尔顿 41
Game of Treize 数十三游戏 337
Games, dynamical 动态游戏 116－129
Games, statical 静态游戏 103－116
Game of mouse trap 捉老鼠游戏 336
Games with counters 筹码游戏 103－105,121－127

我们必须知道，而且我们必将知道

Games with pawns 卒子游戏 124 – 126
Gardner, M. 加德纳 110,112,113
Gauss, C. F. 高斯 26,62,68,75,94,365,373
Genus 亏格 234
Geodesic problems 测地问题 120 – 121
Geography, physical 地文学(即,自然地理) 238
Geometrical fallacies 几何谬论 76 – 84
Geometrical problems, three classical 三个古典的几何问题 338 – 359
Geometrical recreations 几何游戏 76 – 161,312 – 337
Gerbert 热尔贝 351
Gergonne's problem 热尔岗问题 328 – 333
Gerwien, P. 热尔文 89
Ghersi, I. 格尔西 186
Gillies, D.B. 吉利斯 65
Glaisher, J.W.L. 格莱谢尔 167,349
Golay, M. 戈莱 303
Goldbach, C. 哥德巴赫 349
Goldbach's theorem 哥德巴赫定理 64
Goldberg, M. 戈尔德贝格 90,96,155
Golden section 黄金分割 57,132
Golomb, S.W. 戈隆 109
Goormaghtigh, M.R. 古尔马泰 333
Gosset, T. 戈塞特 171
Gradshtein, I.S. 格拉德施坦 67
Grandpré, A. de, 格昂普雷 388
Gray code 格雷码 299
Great dodecahedron 大十二面体 145,234
Great icosahedron 大二十面体 145
Great Northern puzzle 大北方谜题 116,129
Greenwich Labyrinth at 格林威治迷宫 259
Gregory, James. J·格雷戈里 27,348,349,356
Gregory of St. Vincent (圣樊尚的)格雷戈里 343
Gregory's series 格雷戈里级数 356
Greitzer, S.L. 格赖泽尔 28
Grienberger, on π 格林伯格,论 π 355
Grilles 格里尔斯 401
Grinbergs, È, Ya. 格林伯格斯 264 – 265
Gros, L., on Chinese rings 格罗斯,论九连环 320 – 322
Group, Icosahedral 二十面体群 158
Grundy 格伦迪 36
Guarini's problem 瓜里尼问题 189
Guitel, E. 吉特尔 89
Günther, S. 炯特 166,167,194
Guthrie, on colouring maps 格思里,论地图染色 223
Guy, R.K. 盖伊 39

H

Haan, B. de, on π 哈恩,论 π 349,

我们必须知道，而且我们必将知道

http://maths352.bokee.com



354
Hadamard, J. 阿达玛 62,274,296
Haji, T. 哈吉 17
Haken 哈肯 224
Halberstram, H. 哈尔伯斯塔姆 62
Hall, M. 霍尔 278,283
Halley, on π 哈雷,论 π 356
Halmos, P. 哈尔莫斯 50
Hamilton, W. 哈米尔顿 223,262-266
Hamiltonian game 哈密顿博弈 262-266
Hampton Court, maze at 汉普顿宫的迷宫 254,259
Hanoi, tower of 河内塔 316-317
Harber, E.A. 哈伯 40
Hardy, G.H. 哈代 68
Haselgrove, C.B. 哈兹尔格罗夫 111
Heath, T. T·希思 132,134
Heath, R.V. R·V·希思 13,200,201,212,215,221
Heawood, P.J., on maps 希伍德,论地图 224,227-229,232,236-238
Hegesippus, on decimation 赫格西帕斯追述劫难 32
Hein, P. 海因 113
Henry, Ch., on Euler's problem 亨利,论欧拉问题 243
Hero of Alexandria (亚历山大里亚的)希罗 341,351
Herodotus 希罗多塔斯 389
Herodotus, on the labyrinth at Lake Moeris 希罗多塔斯述美利斯湖边的迷宫 256
Herschel, Sir. John J·赫谢尔 368
Herschel, Sir William W·赫谢尔 369
Hess, E. 黑斯 155
Hexagons, interlocked 联棱六边形 215-217
Hilbert, D. 希尔伯特 88,237
Hill, L.S. 希尔 412
Hills and dales 山与谷 238
Hippias 希皮亚斯 350
Hippocrates of Chios (希俄的)希波克拉蒂斯 341,350
Hoist, E. 霍尔斯特 90
Hoppenot, F. 奥普诺 58
Houdin, J.E.R. 乌丹 374
Hudson, C.T. C·T·赫德森 332
Hudson, W.H.H. W·H·H·赫德森 324
Hurwitz, A. 胡尔维茨 40,65
Hutton, C. 赫顿 4,356
Huygens, C. 惠更斯 343,347,355
Hypercubes 超立方体 141
Hypocycloid, three-cusped 三尖内旋轮线 100

I

Iamblichus 伊安布里霍斯 249
Icosahedron, regular 正廿面体 132,238-242,300
Icosahedron, rhombic 廿菱形面体 143
Icosaheadron, stellated 星形廿面体 146-147

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Inaudi, J. 伊瑙迪 375 – 378
Incidence matrix 关联矩阵 272
Infeld, L. 因菲尔德 73
Ingham, A.E. 英哈姆 63,235
Interlocked hexagons 联接六边形 215 – 217
Intermediate convergents 中介渐近分式 87
Inwards on the Cretan maze 殷沃兹,论克雷顿迷宫 257
Ionian School 约恩学派 350

J

Jaenish, C.F. de 耶尼施 173,185
Jephson, T. 杰夫森 368
Johnson, G.O. G·O·约翰逊 66
Johnson, W., on fifteen puzzle W·约翰逊,论十五子戏 312
Jones, W., on π 琼斯,论 π 349, 356
Josephus problem 约瑟夫斯问题 32 – 36
Jotapata 乔塔帕特 32
Julian's Bowers 朱利安的后宫 259
Julius Caesar 凯撒 403

K

Kakeya, S. 挂谷宗一 99,100,101, 102
Kaleidoscope 万花筒 155 – 160
Kamke, E. 卡姆克 44
Kani, E.J.A. 卡尼 ix
Kayles 凯尔斯 39
Kempe, A.B., on colouring maps 肯普,论地图染色 224
Kepler, J. 开普勒 133
Kepler – Poinsot polyhedra 开普勒 – 普安索多面体 133,134,144 – 146, 234
Khajuraho 克久拉霍 203
Kings, I. 金斯 350
King's re – entrant path 王的回路 185
Kirkman, T.P. 柯克曼 ix,281,288
Kirkman's problem 柯克曼问题 287 – 289
Klarner, D.A. 克拉纳 112,113
Klein, F.C. 克莱茵 69,86,237,338
Klein, W. W·克莱茵 386
Klein bottle 克莱茵瓶 237
Knight's re – entrant path 马的回路 174 – 185
Knight of the Round Table 圆桌周围的爵士 49
Knuth, D. 克努特 ix,267,352
Knyghton 克奈顿 256
König, D. 柯尼希 266
Königsberg problem 柯尼希斯堡(即,王堡)问题 243
Kraïtchik, M. 克拉依奇克 13,28, 65,73,95,106,186,200,202,207
Kubota 洼田忠彦 99
Kummer, E.E. 库默尔 71

L

Labosne 拉博斯尼 11
Labyrinths 迷宫 254 – 260
Labyrinth at Boughton Green 布顿格林

我们必须知道，而且我们必将知道

http://maths352.bokee.com

迷宫 259
Labyrinth at Chartres 沙特尔迷宫 259
Labyrinth at Chilcombe 奇尔康贝迷宫 259
Labyrinth at Comberton 康伯顿迷宫 259
Labyrinth at Greenwich 格林威治迷宫 259
Labyrinth at Lucca 卢卡迷宫 258
Labyrinth at Poitiers 普瓦捷迷宫 258
Labyrinth at Ravenna 拉韦纳迷宫 258
Labyrinth at Rockliff Marshes 罗克利夫沼地迷宫 259
Labyrinth at Rome 罗马迷宫 258
Labyrinth at Saffron Walden 萨弗伦沃尔登迷宫 259
Labyrinth at Southwark 索斯沃克迷宫 259
Labyrinth at St. Omer 圣奥默迷宫 259
Labyrinth at Trastevere 特拉斯梯维尔迷宫 258
Labyrinth at Wing 温域迷宫 259
Lacquière 拉奎埃 184
Ladder graph 梯状图 277
Lagny, de, on π 拉尼,论 π 356
Lagrange 拉格朗日 61
La Hire, P. de 拉·伊尔 202,203
La Loubère, S. 拉·卢拜尔 195,204-205
Lambert 兰伯特 347
Lamé, G. 拉梅 71
Landau, E. 兰道 324
Landry, F. 兰德里 68
Latin cubes 拉丁立方 192
Latin squares 拉丁方 189,289-293
Lattice graph 格图 305
Lattice point 格点 86
La Vallée Poussin, C.J.de, 德·拉·瓦莱普桑 62-63
Lavernède, J. E. T. de 拉韦内德 182
Leake 利克 12,17,28
Lebesgue, H. 勒贝格 71,99
Leech, J. 利奇 308
Legendre, A. M. 勒让德 62,71,177,185
Lehmer, D.H. D·H·雷默 viii,55,61,66,72
Lehmer, D.N. D·N·雷默 58
Lehmer's machine 雷默机器 61
Leibnitz, G.W. 莱布尼茨 2,61
Leonardo of Pisa, on π (比萨的)莱昂纳多,论 π 352
Leslie, J. 莱斯利 341,345
Leurechon, J. 勒雷雄 3,12
Life of A. Sharp, by W. Cudworth 卡德沃斯的夏普传 356
Linde, A. van der, 范·德·林德 175
Lindemann, on π 林德曼,论 π 348
Lines of greatest slope 梯度线 238
Lint, J.H. van, 林特 307
Listing, J.B. 利斯廷 128,244
Littlewood, J.E. 李特尔伍德 63
Lobachevsky, N.I. 罗巴契夫斯基 280

我们必须知道，而且我们必将知道



London, W. and Wise 伦敦与怀斯 259
Longuet－Higgins, M.S. 隆盖-希金斯 146
Lo－sho 洛书 196
Loubère, S. De la 卢拜尔 195,204－205
Loyd, S. 劳埃德 29,39
Lucas, E. 吕卡斯 50,59,65,119,124,125,145,189

M

Macaulay, W.H. 麦考利 93
Macclesfield 麦克尔斯菲尔德 356
Machin's series for π π的梅欣级数 356
MacLane, S. 麦克莱恩 73
MacMahon, P.A. 麦克马洪 113
MacNeish 麦克尼希 293
Magic cubes 魔立方 217－221
Magic squares 幻方 193－221
Major MacMachom 大麦克马洪 51
Mallison, H.V. 马利森 313
Mangiamele, V. 曼伽美尔 372
Mann, H.B. 曼恩 297
Map colour theorems 地图染色定理 222－231,235－237
Margossian 马戈西安 208,221
Mars 马尔斯 297
Mascheroni, L. 马歇罗尼 96,97
Maxwell, J.C. 麦克斯韦 6,238
Mayan glyphs 马雅象形文字 417
Mazes 迷宫 254－260
McClintock, E. 麦克林托克 203
Medema, P. 米德马 116
Medieval problems 中世纪的问题 27－36
Menaechmus 梅内克缪斯 342
Ménage problems 梅纳热问题 27－36
Mendelsohn, C.J. 门德尔松 413
Menon, P.K. 梅农 293
Mersenne's numbers 默森数 xii,65
Mesolabum 连比中量法 341
Metius, A., on π 梅蒂尤斯,论π 353
Méziriac 梅齐里亚克 3
Mikami, Y. 三上义夫 201
Miller, G.A. G·A·米勒 279
Miller, J.C.P. J·C·P·米勒 ix,53,138,146,153
Milton 弥尔顿 386
Minding 明金格 185
Mineur, A. 米诺 90
Minos 米诺斯 254,340
Minotaur 米诺陶 257
Mirrors 镜子 155－161
Missing digits 丢失的数码 20－26
Mitchell, F.D. 米切尔 363,374
Möbius, A.F. 麦比乌斯 128,159
Möbius strip 麦比乌斯带 128,237
Models, geometrical 几何模型 130,134,153,158
Mohammed's sign manual 穆罕默德签署 248
Mohr, G. 莫尔 96
Moivre, A. de, 德莫瓦夫尔 （见"棣莫弗"） 175

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Mondeax, H. 蒙塞 372,377

Mondovi 蒙多维 27

Monge, on shuffling cards 蒙日,论洗牌 323

Monoalphabetic systems 单字母法 404

Montmort, de 蒙特莫尔 2,46,176

Montucla, J.E. 蒙蒂克拉 4,89,347,355,176

Moon 穆恩 185

Moore, E.H. 穆尔 38,278

Mordell, L.J. 莫德尔 69

Morehead, J.C. 莫尔黑德 68

Morgen, A. de 德·摩根 223,347,349,359

Moroń, Z. 莫龙 115

Morrison, M.A. 莫里森 68

Morse 莫尔斯 388

Morse code 莫尔斯电码 406

Mosaic pavements 马赛克铺砌 107,266-269

Moschopulus 摩绍普拉斯 194

Mulder, P., on Kirkman's problem 米尔德,论柯克曼问题 288

Müller, G.E. G·E·缪勒 360-378

Muncey, J.N. 芒西 211

Mydorge, C. 米多尔热 3

N

Napoleon 拿破仑 27

Nasik *magic squares* 纳西克幻方(即超幻方,或至美幻方、魔幻方) 203,206,208-212

Nauck, F. 瑙克 166

Naville, E.H. 纳维尔 98

Newbold, W.R. 纽博尔德 417

Newman, D.J. 纽曼 50

Newton, I. 牛顿 343,344,346

New York Times 纽约时报 294

Nicholas, C. de Cusa 尼古拉斯 353

Nicomedes 尼科米迪斯 341

Nim 尼姆 36-38

Nine digits problem 九数码问题 15,40

Non-orientable surface 不可定向曲面 232

Normal piling 规范垒装 149,151

Naughts and crosses 圈与叉 104

Numbers, perfect 完全数 66-67

Numbers, puzzles with 数字游戏 4-50

Numbers, theory of 数论 57-75,231

O

O'Beirne, T.H. 奥贝恩 39,359

Octahedron 八面体 132,147,215

Oppert, on π 奥佩尔,论 π 350

Orientability of surfaces 曲面的可定向性 232

Osgood 奥斯古德 99

Otter, R.E. 奥特 261

Oughtred 奥特雷德 349

Oughtred's Recreations 奥特雷德游戏 12,17,28

Ovide 奥维德 256

Ozanam, A.F., on labyrinth 奥札南,论迷宫 258

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Ozanam's Recreations 奥札南游戏 3,4,12,28,85,118,176,191,318

P

π 347 – 359

Pacioli di Burgo (伯尔诺的)帕乔利 3

Pairs – of – cards trick 牌对游戏 326 – 328

Pál, J. 帕尔 99

Paley, R.E.A.C. 佩利 108,309

Pandiagonal magic squares 泛对角幻方 203,206,208 – 212

Pan – Kai 盘凯 111

Pappus 帕普斯 134,341,345

Paradromic rings 并环 127,232

Parker, E.T. 帕克 292

Parmentier, on Knight's path 帕门蒂埃,论马路 175

Pars, L.A. 帕尔斯 227 – 230

Parville, de 帕尔维伊 317

Patz, W. 帕茨 55

Paxson, G.A. 帕克森 69

Pentagram 五芒星形 144,248

Pepys, S. 佩皮斯 389

Perelman 彼列尔曼 40

Perfect code 完备码 276

Perfect magic square 至美幻方 203,206,208 – 212

Perfect numbers 完全数 66 – 67

Perigal, H. 佩里伽尔 88

Permutation problems 排列问题 48 – 50,312 – 326

Pervusin, I.M. 佩尔武申 65

Petersburg paradox 圣彼得堡悖论 44

Paterson, A.C. A·C·彼得森 305,373

Peterson, J., on graphs J·彼得森,论图 226,305

Petrie, J.F. 皮特里 147,153,157,135

Petrie polygon 皮特里多角形 135,145

Philo 菲洛 341

Philoponus, on Delian problem 菲洛波纳斯,论德利安问题 339

Photo – electric number – sieve 光电数字筛 61

Physical geography 自然地理(即,地文学) 238

Piet Hein 皮特·海茵 113

Pirie, G., on π 皮里,论 π 355

Pile problems 堆垒问题 328 – 333

Pits, peaks, and passes 峰顶、谷底、鞍点 238

Planck, C. 普朗克 203,210,310

Plane of Symmetry 对称平面 131,136

Planets 行星 194

Platonic solids 柏拉图体 130 – 135,238

Plato, on Delian problem 柏拉图,论德里安问题 339 – 342

Playfair cipher 公允式密码 410

Pliny 普利尼 256

Poinsot 普安索 134

Pole, W. 波耳 385

Polignac, A. de, 德·波利尼亚克

我们必须知道，而且我们必将知道

http://maths352.bokee.com



64,184

Pollock, B.W. 波洛克 71

Polyalphabetic systems 复式字母法 406 - 410

Polygraphic substitutions 字母组替换法 410 - 412

Polyhedra 多面体 130 - 161

Pólya, G. 波伊亚 106,161,261

Polyliteral systems 多字法 406

Polyominos 多方联(多米诺,超级骨牌) 109 - 113

Portier, B., on magic squares 波尔捷,论幻方 212

Posner, E.C. 波斯纳 297

Poussin, De la Vallée 德·拉·瓦莱·普桑 62 - 63

Powers, R.E. 鲍尔斯 65

Pratt, on knight's path 普拉特,论马路 181

Prime pairs 素数偶 64

Primes 素数 60 - 66,211

Probabilities 概率 44 - 48,84,337,359

Projective planes 射影平面 234 - 236,271,310

Ptolemy 托勒密 351

Purbach, on π 普尔巴赫,论 π 352

Puzzles, arithmetical 算术趣题 4 - 52

Puzzles, geometrical 几何趣题 77 - 128

Pyramidal numbers 金字塔数 59,149

Pythagoras 毕达哥拉斯 350

Pythagoras' theorem 毕达哥拉斯定理 57,88

Pythagoreans 毕达哥拉斯学派 249

Q

Qudratic residues 二次剩余 108

Quadrature of circle 化圆为方 347 - 359

Queens problem, eight 八后问题 166 - 171

Queens, problems with 后的问题 189

R

Raghavarao, D. 拉伽瓦诺奥 309

Ramification 分歧 260 - 262

Ray - Chandhuri, D.K. 雷-钱杜瑞 288

Reciprocal polyhedra 反多面体 134 - 136,152,234

Reciprocal tessellations 反铺砌 107

Re - entrant chess paths 棋子回路 175 - 188

Reflexible figures 自反的图形 130,138

Regiomontanus, on π 雷格蒙塔努斯,论 π 353

Regular polygons 正多边形(正多角形) 131

Regular polyhedra 正多面体 131

Regular sponges 正海绵胞 152 - 153

Regular tessellations 正则铺砌 105,134,152,266

Reimer, N.T. 赖默 339

Reiss, M. 赖斯 127,254

Renton, W. 任顿 84

Residues 留数 60,108

我们必须知道,而且我们必将知道

http://maths352.bokee.com

Restoration of digits 数码补复 20 - 26
Reynolds, O. 雷诺 151
Rhind papyrus 莱因德莎草纸书 350
Rhombicuboctahedron 立方八菱面体 137
Rhombicosidodecahedron 二十 - 十二菱面体 137
Rich, J. 里奇 389
Richmond, H.W. 理奇蒙德 95
Richter, on π 黎赫特,论 π 358
Riemann, G.F.B. 黎曼 63,75
Riesel, W. 里塞尔 65
Right - angled triangles 直角三角形 57,58
Rilly, A. 里利 185,212
Ringel, G. 林格尔 x,238
Rivest 里韦斯特 112
Robert - Houdin, J.E. 罗伯特乌丹 374
Robinson, G.de B. G·de B·鲁宾逊 159
Robinson, R.M. R·M·鲁宾逊 64,65,69
Rodet, L., on Calculus of Arya-Bhata 罗德,著:阿耶波多演算 351
Roget, P.M. 罗热 175,179 - 185
Romanus, on π 罗曼努斯,论 π 353
Rook's re - entrant path 车的回路 187
Rosamund's Bower 罗莎蒙德的闺房 256
Rosen, F., on Arab value of π 罗森,论 π 的阿拉伯值 342
Rosser, J.B. 罗瑟 72,203,219,204
Rotating rings of tetrahedra 四面体的旋转环 153,215,234
Roth, K.F. 罗特 62
Round table, knights of the 圆桌骑士 49
Routes on chess - board 棋盘上的路线 175 - 188
Rückle, C. 吕克勒 375 - 378
Rudio, F., on π 鲁迪奥,论 π 347
Running - Key system 流动密钥法 410
Rutherford, on π 卢瑟福,论 π 357
Ryser, H.J. 赖瑟 311

S

Safford, T.H. 萨福德 374
St. Laurent, de, on cards 圣洛朗,论牌 323
St. Petersberg paradox 圣彼得斯堡悖论 44
St. Vincent, Gregory of 圣樊尚的格雷戈里 343
Sauveur, J. 索弗尔 203
Sayles, H.A. 塞尔斯 211
Scale of notation, denary 十进制 10 - 17
  Transforming to another 进位制的转换 55,352
Schläfli, L. 施勒夫利 141,146
Schoenberg, I.J. 舍恩贝格 101,102
Shots, M.H. 绍茨 212
Schubert, H., on π 舒伯特,论 π 347

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Schuh, H. 舒 22

Schumacher, H.C. 舒马赫 373

Scripture, E.W. 斯克里普丘 360

Secret communications 秘密通讯 388 - 418

Seidel, J.J. 赛德尔 viii, 307

Selander, K.E.J., on π 塞兰德，论 π 349

Selberg, A. 赛尔伯格 62 - 63

Selfridge, J.L. 塞尔弗里奇 ix, 62, 69, 71

Seven - colour map theorem 七色地图定理 237

Shakespeare 莎士比亚 417

Shanks, W., on π 尚克斯，论 π 357, 386

Sharp, A. 夏普 129, 143, 356

Shelton, J. 谢尔顿 389

Sherwin's table 舍温表 356

Shrikhande, S.S. 施瑞克罕德 292

Shuffle board 掷盘戏(或推盘戏) 196

Shuffling cards 洗牌 323 - 325

Shuldham, C.D. 舒尔德海姆 211

Shunting problems 调车问题 116 - 118

Shunting, railway puzzle 调车趣题 116 - 118

Singer, J. 辛格 286

Sinkov, A. 辛科夫 vii

Sixty - five puzzle 六十四变六十五 85

Skeleton cube 立方骨架 295

Smith, A., on π A·史密斯，论 π 354

Smith, C.A.B. C·A·B·史密斯 39, 115, 265 - 266

Smith, D.E. D·E·史密斯 196, 201, 203, …

Smoke - ring 烟圈 154

Snell, W., on π 斯内尔，论 π 354

Snub solids 扭棱体 139

Solitaire 单人跳棋 103, 127

Soma 立体拼装 112

Sommerville, D.M.Y. 萨默维尔 141

Space - filling curve 充满空间的曲线 269

Spherical close - packing 球体密装 149, 151

Sporus, on Delian problem 斯波拉斯，论德利安问题 343

Sprague, R. 斯普拉格 36, 115

Sprague - Grundy number 斯普拉格 - 格伦迪数 36 - 37, …

Squaring the circle 化圆为方 347 - 359

Squaring the rectangle 剖矩成方 115

Stalker, R.M. 斯托克 154

Standard alphabets 标准字母 403

Stark, H.M. 斯塔克 60

Star - pentagon or pentagram 五芒星 144

Staudt, K.G.C. von, 冯·施陶特 271, 282

Stauton 斯汤顿 165

Steen, on the Mouse Trap 斯蒂恩，论老鼠夹子 336

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Steiner, J. 施泰纳 278,288,310
Steiner triple systems 施泰纳三元组 278－289,…
Steinhaus, H. 施泰因豪斯 232,238
Steinitz, E. 施泰尼茨 136
Stella octangula 八芒星 135,136,146
Stellated polyhedra 星形多面体 144－146
Stone, A.H. 斯通 115
Storey, on the fifteen puzzle 斯托里,论十五子戏 312
Stott, Mrs. 斯托特夫人 139
Strabo, on the labyrinth at Lake Moeris 斯特拉波,关于美利斯湖边的迷宫 256
Strachy, R. 斯特雷奇 196
Strasznicky 斯特拉斯尼斯基 373
String figures 结绳图 vii
Sturm, A. 斯图谟 339
Sub－factorial 次阶乘 47
Substitution 代换 402－414
Suetonius 雪托尼厄斯 403
Super－dominoes 超级骨牌 109－113
Surfaces, unbounded 无边曲面 232
Swastika 卍(古吉祥图案,读作"万") 258
Swinden, B.A. 斯温丹 36
Sylvester, J.J. 西尔维斯特 67,104,296
Symmetrical magic squares 对称幻方 202
Symmetry 对称 130,135,151

T

Tait, P.G. 泰特 34,123,128,224－227,230－231,244
Tanner, L., on shuffling cards 坦纳,论洗牌 323
Tarry, G. 塔里 x,120,192,212,249－256,292
Tartaglia 塔尔塔利亚 3,28,33,56,118
Taylor, B. B·泰勒 176
Taylor, Ch. C·泰勒 346,…
Taylor, H.M. H·M·泰勒 92,163,…
Ten digits problem 十个数码的问题 15,40
Tesselation, plane 平面铺砌 105－116,155,266
Tesselation, solid 立体拼砌 147－152,159
Tetrahedral numbers 四面体数 59
Tetrahedron 四面体 132,148
Texeira, F.G. 特谢拉 338
Theaetetus 西艾泰德斯 132
Theory of numbers 数论 57－75,231
Thibaut, G., on Baudhayana 蒂博,述鲍德海雅纳 351
Three－in－a－row 三子成行 104
Three－pile problem 三摞问题 328
Todd, J. 托德 358
Torus 环面 216,222,237
Tower of Hanoi 河内塔 316,317
Travers, J. 特拉弗斯 93,201
Trebly－magic squares 三重幻方 213

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Trees 树 260 - 262
Tremaux 特雷莫 x
Triacontahedron 三触面体 137
Triangular graph 三角形图 304
Triangular number 三角形数 59
Trick with numbers 数字把戏 4 - 50
Trisection of angle 三等分角 344 - 347
Troitsky 特罗伊茨基 14
Trollope, E., on maze 特罗洛普,论迷宫 257
Troy - towns 特洛伊城 259
Truncated solids 截顶体 138, 147, 153
Tsu Ch'ung-chih 祖冲之 352
Tuckerman, B. B·塔克曼 65,67
Tuckerman, L.B. L·B·塔克曼 242
Turton, W.H. 特顿 81,174
Tutte, W.T. 塔特 ix,115,264
Two-digit process 双位法 381

U

Uniform polyhedra 匀称多面体 136, 159

V

Valerio, P. 瓦莱里奥 404,418
Vallée - Poussin, Ch.J. de la 瓦莱 - 普桑 62 - 63
Van Ceulen, on π 范柯伦,论 π 353
Vandemonde, A.T. 范德蒙特 127, 175,180,181
Vandiver, H.S. 范迪维尔 71
Van Etten, H. 范埃滕 12
Vase problem 分油问题 28
Vaughan, H.E. 沃恩 50
Veblen, O 维布伦 207,282
Vega, on π 维伽,论 π 357
Vegenère 维热奈阿 407
Vieta, F. 韦达 343,353
Vigenère Square 维热奈阿正方表 407,409
Vinogradoff, L.A. 维诺格拉多夫 64
Virgil 维吉尔 256,386
Volpicelli, P., on knight's path 沃尔皮契礼,论马路 175
Von Bilger, on chess pieces 冯·比尔格,论棋子 165
Voting 投票 49,106
Voynich, W.M. 沃伊尼克 417

W

Walker, G.T. G·T·沃克 41
Walker, R.J. R·J·沃克 203,204, 219
Wallis, J. 沃利斯 318,355,361
Wantzel, P.L. 旺策尔 94,338
Warnsdorff, on knight's path 沃恩斯道夫,论马路 175,181
Watch problem 钟表问题 17
Watersheds and watercourse 分水岭与溪床 238
Watson, G.N. 沃村 59
Weight problem 砝码问题 50
Weil, A. 韦伊 75
Wenzelides 文策莱德斯 185
Western, A.E., on binary powers 韦斯顿,论二的幂 68

我们必须知道，而且我们必将知道

http://maths352.bokee.com

Whateley, R.　惠特利　365
Wheeler, A.M.　惠勒　93,94,147
White, A.S.　怀特　281
Whittaker, E.　惠特克　386
Wiedermann, A., on the labyrinth at Lake Moeris　威德曼,论美利斯湖边的迷宫　256
Wieferich, A.　威斐礼奇　71
William, H.B.　威廉　213
Wythoff, W.A.　威索夫　39,159
Willcocks, T.H.　威尔科克斯　115
Wilson, J.C.　J·C·威尔逊　61,116,244
Wilson, R.M.　R·M·威尔逊　288
Wilson's theorem　威尔逊定理　61
Window reader　窗口里瞧　333－336
Winn, C.E.　温　230
Winter, F.　温特　113
Wright, E.M.　赖特　68

Y

Yardley, H.O.　亚德利　418
Yates, F.　耶茨　192
Youngs, J.W.T.　扬斯　ix,238
Yu　禹(即,夏禹王)　196

Z

Zach, F.X. von, on π　冯察赫,论 π　357
Zamebone, U.　扎姆博恩　375
Zeller　泽勒　26
Zeta function　ζ-函数　63
Zonohedra　环带多面体　141

我们必须知道，而且我们必将知道

http://maths352.bokee.com

关于本书

八十年来，这本赏心悦目的上乘作品以数学话题或俗说的游戏向人们提供了消遣与享受.虽然这些题材常包含着基本的数学方法和概念，但其主要的引人入胜之处在于它们是以游戏和哑谜出现而不在于其结论的实用性.

这本新版(第12版)保持了原貌，不过术语和问题的处理已予以更新，并且增添了许多新的内容. 其中有关于多米诺骨牌与龙纹设计的新节段和一整章“组合论”入门. 全书述及的其他话题还有数字游戏与几何游戏、多面体、棋盘上的游戏、魔方、地图染色问题、一笔画线问题、密码编制与密码破译、以及计算神童小传等.

由于不需要微积分和解析几何的知识就可以欣赏这些娱乐节目，这本书很适合广大数学师生们以及任何对数学有点兴趣的读者的需求.

罗斯·鲍尔(1850—1925)还著有数学方面的其他著作，包括《数学简史》(Short History of Mathematics)与《剑桥数学研究史》(History of the Study of Mathematics at Cambridge).

H·S·M·考克塞特为多伦多大学教授.

我们必须知道，而且我们必将知道